Q: Who is a Global Military Defense Cyber Space Intelligence and AI Analyst ? Kindly Define and Elaborate ? What is the nature of the job ?

A: Starts with a Biological Entity explaining who or what is an Analyst followed by Machine Neural Network Generative AI's take on the rest.

Some essential elaboration on who or what is an 'ANALYST' ?

Advanced human modified and elaborate lexicon grade definition :

Someone who is skilled at considering in detail a subject inorder to discover essential features or meaning through vigorous and robust study. May require mathematical and grammatical analysis to break down or dissect the essential components and features. Sometimes , may include elements from the diverse domains of psychoanalytics. Othertimes , the Analyst may recommend appropriate operational , tactical or strategic recommendations to Global Agencies , Organisations and Governments in line with the International order.

As a Transitive Verb it means to study or determine the nature and relationship of the parts of (something) by analysis subject to modern scientific and grammatical deliberations. An analytical mind thinks and broods in the opposite direction of a synthetic one. Establishes reasoning to distinguish , differentiate the unique identities of all the

constituent parts . Starting the process idealistically ,

progressing theoretically and arriving pragmatically in comprehending useful associations between intricate and complex issues. Natural decomposition of a hypothesis or theory into smaller self contained and connected parts inorder to elucidate a seeming perplex large entity is the obvious approach that most Human Analysts would want to adopt for apparent methodical reasons. Logically , they deduce the proof from known truths just the way symbolic logic of boolean algebra , developed by George Boole , applies to computer programs .

But when doing the same mathematically , the broad field of study (often mentioned alongside algebra) which developed out of calculus, concerned with the behavior of functions, sequences, series, limits, metric spaces, measures and more.

Interestingly , when the military uses concise verbiage ; in the English Language , 'ANALYSE' bonds them together , beautifully as per the laws of phraseology and enunciation at least .

Verb:
analyse (analyses, present participle : analysing; simple past and past participle : analysed)

Standard spelling of 'analyze'.

History and Etymology :

Borrowed from French analyste "mathematician skilled in analysis," probably by haplology from *analysiste, from analyse or analysie analysis.

NOTE: French analyste would appear to be a derivative of analyser, a counterpart to analyze in English, but the French verb is apparently attested several decades later than the agent noun.

Global Military Defense Cyber Space Intelligence and AI Analyst explained by Gemini , Chatgpt and Grok.

Google Gemini

A Global Military Defense Cyber Space Intelligence and AI Analyst is a specialized professional who focuses on understanding and mitigating threats in the cyber domain that could impact military operations, defense infrastructure, and national security on a global scale. This role uniquely integrates expertise in cybersecurity, intelligence analysis, and artificial intelligence to provide critical insights and support strategic decision-making within military and defense organizations.
Here's a breakdown of the definition and elaboration:
Definition:
A Global Military Defense Cyber Space Intelligence and AI Analyst is responsible for identifying, analyzing, and predicting cyber threats and vulnerabilities targeting military assets, personnel, and operations worldwide. They leverage

intelligence gathering methodologies, cybersecurity principles, and artificial intelligence tools to provide actionable insights that enhance cyber defense strategies, inform decision-makers, and contribute to the overall security posture of military forces in the cyberspace domain.
Elaboration:
This multifaceted role involves several key areas of expertise and responsibility:
* Cyber Space Expertise: Possesses a deep understanding of the cyber domain, including network architectures, protocols, operating systems, cybersecurity technologies (firewalls, intrusion detection/prevention systems), and common attack vectors. They are familiar with the tactics, techniques, and procedures used by state-sponsored actors, cybercriminal groups, and other malicious entities in cyberspace.
* Intelligence Analysis: Applies intelligence analysis principles to collect, evaluate, and interpret information related to cyber threats. This includes open-source intelligence (OSINT), signals intelligence (SIGINT), and potentially classified information. They are skilled in identifying patterns, trends, and indicators of malicious cyber activity and in assessing the intent and capabilities of cyber adversaries.
* Artificial Intelligence (AI) and Machine Learning (ML): Utilizes AI and ML techniques to enhance cyber threat detection, analysis, and prediction. This can involve developing and deploying AI-powered tools for anomaly detection, malware analysis, threat intelligence gathering, and automated incident response. They understand the application of AI in both offensive and defensive cyber operations and can analyze AI-driven threats.

* Global Perspective: Maintains awareness of the global cyber threat landscape, including geopolitical factors, international cyber policies, and the cyber capabilities of different nations and non-state actors. They understand how global events and trends can influence cyber threats against military and defense interests.
* Threat Intelligence: Collects, processes, analyzes, and disseminates cyber threat intelligence to relevant stakeholders. This includes producing timely and accurate reports, briefings, and assessments that inform strategic and tactical decision-making. They understand different types of cyber threat intelligence (strategic, tactical, technical, and operational).
* Vulnerability Analysis: Identifies and analyzes vulnerabilities in military cyber systems and infrastructure that could be exploited by adversaries. This may involve using penetration testing tools and techniques or analyzing security assessments and reports.
* Incident Response Support: Provides intelligence support during cyber incidents, helping to understand the nature of the attack, identify the actors involved, and assess the potential impact. They may contribute to containment, eradication, and recovery efforts.
* Strategic Planning Support: Contributes to the development of long-term cyber defense strategies and policies based on their understanding of the evolving threat landscape and emerging technologies.
* Collaboration and Communication: Works closely with other cybersecurity professionals, intelligence analysts, military personnel, and policymakers. They must be able to communicate complex technical information clearly and

effectively to both technical and non-technical audiences.
Nature of the Job:
The nature of the job is typically demanding and requires a high level of technical expertise, analytical skills, and attention to detail. It often involves:
* Continuous Learning: The cyber threat landscape and AI technologies are constantly evolving, requiring ongoing professional development and staying abreast of the latest trends and threats.
* Problem Solving: Identifying and analyzing complex cyber threats and developing effective countermeasures requires strong problem-solving skills.
* Critical Thinking: Evaluating information from various sources, discerning patterns, and making informed judgments are crucial aspects of the role.
* Working Under Pressure: Responding to cyber incidents and producing timely intelligence often requires working under tight deadlines and high-pressure situations.
* Ethical Considerations: Maintaining the highest ethical standards is paramount, especially when dealing with sensitive information and potentially contributing to offensive cyber operations (depending on the specific role).
* Potential for Classified Work: Depending on the employing organization and specific responsibilities, the role may involve handling classified information and requiring security clearances.
* Collaboration: Working as part of a team and collaborating with individuals from diverse backgrounds and expertise is essential.
* Report Writing and Briefing: Communicating findings and recommendations through written reports and oral briefings

is a significant part of the job.
In essence, a Global Military Defense Cyber Space Intelligence and AI Analyst acts as a critical guardian in the digital realm, protecting military interests from sophisticated cyber threats by leveraging intelligence insights and the power of artificial intelligence on a global scale.

OpenAI ChatGpt

A Global Military Defense Cyber Space Intelligence and AI Analyst is a highly specialized professional who operates at the intersection of military strategy, cybersecurity, intelligence gathering, and artificial intelligence (AI)—with a global perspective. This role exists primarily within defense agencies, military intelligence units, and global security firms, and is essential in the modern digital battlefield where threats are increasingly cyber-based and AI-driven.

Definition

A Global Military Defense Cyber Space Intelligence and AI Analyst is a subject matter expert who analyzes global military threats and defense strategies, particularly in cyberspace, by using advanced cyber intelligence techniques and artificial intelligence tools. Their primary objective is to secure national or allied interests from cyber warfare, espionage, and AI-driven attacks.

Key Responsibilities

1. Cyber Threat Intelligence:

Detect, monitor, and analyze cyber threats from state and non-state actors.

Identify patterns, tactics, techniques, and procedures of adversaries.

2. AI-Powered Analytics:

Use machine learning, neural networks, and data mining to process large datasets (e.g., satellite feeds, signals intelligence, malware behavior).

Develop predictive models to foresee threats or potential security breaches.

3. Military Intelligence Fusion:

Integrate data from HUMINT, SIGINT, IMINT, and OSINT with cyber threat intelligence.

Advise military command structures on possible courses of action.

4. Cybersecurity Operations:

Conduct vulnerability assessments and penetration tests on military networks.

Assist in cyber defense operations and threat mitigation strategies.

5. Strategic Defense Planning:

Contribute to the development of cyber defense doctrines and AI warfare strategies.

Provide input for digital warfare simulations and readiness exercises.

6. International Collaboration:

Liaise with NATO, UN cyber units, and allied nations on defense intelligence sharing.

Monitor global geopolitical cyber dynamics.

Nature of the Job

High-security clearance is often required.

Work environment includes classified operations centers, war rooms, and digital forensics labs.

Cross-disciplinary skills are essential: AI/ML expertise, cyber law, military strategy, and geopolitical analysis.

Stressful and time-sensitive, especially during active threats or geopolitical crises.

May involve 24/7 operations, remote deployments, or coordination with battlefield operations.

Required Background

Degrees in Computer Science, Cybersecurity, Data Science, International Relations, or Military Studies.

Certifications like CISSP, GIAC, or Certified Ethical Hacker (CEH).

Military or intelligence agency training is highly valued.

Experience with AI frameworks (e.g., TensorFlow, PyTorch), SIEM tools, and digital signal processing.

GROK

A **Global Military Defense Cyber Space Intelligence and AI Analyst** is a specialized professional who operates at the intersection of cybersecurity, military defense, intelligence analysis, and artificial intelligence (AI). Their role focuses on leveraging advanced technologies, data analysis, and strategic insights to protect national or global security interests in cyberspace, while also addressing threats and opportunities posed by adversaries in the digital and physical domains. This role is critical in modern warfare and defense, given the increasing reliance on cyber infrastructure and AI-driven systems.

Definition
This analyst is responsible for:
- **Monitoring and analyzing cyber threats** targeting military and defense systems, including networks, weapons systems, and critical infrastructure.
- **Gathering and interpreting intelligence** from cyber activities, open-source data, signals intelligence (SIGINT), and other sources to assess adversaries' capabilities,

intentions, and strategies.
- **Utilizing AI and machine learning** to process vast datasets, detect anomalies, predict threats, and enhance decision-making in real-time.
- **Developing strategies** to strengthen cyber defenses, mitigate risks, and ensure operational resilience in contested digital environments.
- **Collaborating with global stakeholders**, including military commands, intelligence agencies, private sector partners, and international allies, to share threat intelligence and coordinate responses.

Elaboration on the Role
The role is multidisciplinary, combining expertise in cybersecurity, military strategy, intelligence tradecraft, and AI technologies. Analysts work in high-stakes environments where cyber operations can have immediate impacts on national security, military operations, and global stability. They must stay ahead of rapidly evolving threats, such as state-sponsored cyberattacks, ransomware targeting defense infrastructure, or AI-driven disinformation campaigns.

Key responsibilities include:
1. **Threat Intelligence Analysis**:
   - Collect and analyze data from cyber intrusions, malware, phishing campaigns, or advanced persistent threats.
   - Identify patterns, tactics, techniques, and procedures used by adversaries, such as nation-states, terrorist groups, or cybercriminals.
   - Use tools like SIEM (Security Information and Event Management) systems, threat intelligence platforms, and AI-

driven analytics to process data.

2. **AI and Machine Learning Integration**:
   - Develop or deploy AI models to detect cyber threats, automate threat hunting, or simulate adversary behavior.
   - Use AI for predictive analysis, such as forecasting potential attack vectors or vulnerabilities in military systems.
   - Ensure AI systems used in defense (e.g., autonomous drones, decision-support tools) are secure from manipulation or adversarial AI attacks.

3. **Cyber Defense Strategy**:
   - Design and implement countermeasures, such as intrusion detection systems, encryption protocols, or zero-trust architectures, to protect military networks.
   - Conduct red teaming (simulated attacks) and blue teaming (defensive operations) to test system resilience.
   - Advise on policies and frameworks for cyber warfare, including rules of engagement in cyberspace.

4. **Global Collaboration**:
   - Work with organizations like NATO, Five Eyes intelligence alliances, or cybersecurity firms to share intelligence and coordinate responses.
   - Participate in joint exercises or simulations to prepare for large-scale cyber conflicts.
   - Stay informed about global trends in cyber warfare, AI advancements, and geopolitical developments.

5. **Incident Response and Recovery**:
   - Lead or support responses to cyber incidents, such as data breaches or denial-of-service attacks on military

systems.
  - Conduct forensic analysis to determine the scope, impact, and attribution of attacks.
  - Develop recovery plans to restore operations while minimizing damage.

Nature of the Job
The nature of this job is **dynamic, high-pressure, and intellectually demanding**. Analysts operate in a fast-paced environment where decisions can have far-reaching consequences for national security. The job involves:

- **Technical Expertise**: Proficiency in cybersecurity tools (e.g., Wireshark, Splunk, FireEye), programming (e.g., Python, R), and AI frameworks (e.g., TensorFlow, PyTorch). Knowledge of military systems, such as command-and-control networks or satellite communications, is often required.
- **Strategic Thinking**: Analysts must translate technical findings into actionable intelligence for military leaders, policymakers, or operational commanders.
- **Continuous Learning**: The cyber threat landscape and AI technologies evolve rapidly, requiring constant upskilling and awareness of emerging tools and techniques.
- **Ethical and Legal Considerations**: Analysts must navigate complex legal frameworks, such as international laws on cyber warfare, and ethical dilemmas, such as balancing offensive and defensive cyber operations.
- **Global Perspective**: The role demands an understanding of geopolitical dynamics, as cyber threats often originate from state actors or non-state actors with global reach.

- **Shift Work and Crisis Response**: Analysts may work irregular hours, including nights and weekends, especially during active cyber incidents or military operations.

Work Environment
- **Settings**: Analysts typically work in secure facilities, such as military bases, intelligence agencies (e.g., NSA, DIA), or defense contractors' offices. Some roles involve field deployments to support active operations.
- **Collaboration**: The job requires close coordination with cybersecurity engineers, data scientists, military officers, and policymakers.
- **Security Clearances**: A high-level security clearance (e.g., TS/SCI in the U.S.) is usually required due to access to classified information.

Skills and Qualifications
- **Education**: A degree in cybersecurity, computer science, data science, international relations, or a related field. Advanced degrees (e.g., MS, PhD) in AI or cybersecurity are increasingly valued.
- **Technical Skills**: Expertise in network security, penetration testing, AI/ML algorithms, and data analytics.
- **Soft Skills**: Strong communication, critical thinking, and problem-solving abilities to convey complex findings to non-technical stakeholders.
- **Certifications**: Relevant certifications include CISSP, CEH, OSCP, or AI-specific credentials like those from AWS or Google.
- **Experience**: Prior work in military intelligence, cybersecurity operations, or AI development is often

preferred.

Challenges

- **Evolving Threats**: Keeping pace with sophisticated adversaries who use AI, quantum computing, or novel attack methods.
- **Information Overload**: Managing and prioritizing vast amounts of data from multiple sources.
- **Attribution**: Determining the origin of cyberattacks, which can be obscured by proxies or false flags.
- **Ethical Dilemmas**: Balancing offensive cyber capabilities with the risk of escalation or collateral damage.

Impact and Importance
This role is pivotal in safeguarding military and national interests in an era where cyberspace is a primary battlefield. Analysts not only protect critical systems but also enable proactive measures, such as disrupting enemy operations or countering disinformation. Their work directly supports mission success, from securing supply chains to ensuring the reliability of autonomous systems in combat.

Conclusion
A Global Military Defense Cyber Space Intelligence and AI Analyst is a hybrid expert who blends cybersecurity, intelligence, and AI to address complex threats in the digital domain. The job demands technical prowess, strategic insight, and global awareness, with a direct impact on military readiness and national security. It is a challenging yet rewarding career for those passionate about defending against 21st-century threats in an increasingly interconnected

world.

Some Real World Instances of Global Platforms , Agencies ,

Organisations, Thinktanks from the domains and verticals of Military , Cyber , Space and AI , proactively involved in the above :

STOCKHOLM INTERNATIONAL
PEACE RESEARCH INSTITUTE.

https://www.sipri.org

United Nations Institute for disarmament research – https://unidir.org/

International Atomic Energy Agency
https://www.iaea.org/

Bulletin of the Atomic Scientists

https://thebulletin.org/

The Cipher Brief – https://www.thecipherbrief.com/

Defense News – https://www.defensenews.com/

Jane's Defence Weekly – https://www.janes.com/

C4ISRNET – https://www.c4isrnet.com/

Breaking Defense – https://breakingdefense.com/

Military Times – https://www.militarytimes.com

Military.com – https://www.military.com/

DefenseScoop – https://defensescoop.com/

Axios – https://www.axios.com/

Modern War Institute – https://mwi.westpoint.edu/

Defense Post – https://thedefensepost.com/

Defense One – https://www.defenseone.com/

War on the rocks – https://warontherocks.com/

Belfer Center – https://www.belfercenter.org/

The RAND Corporation is a nonprofit global policy think tank first formed to offer research and analysis to the United States Armed Forces – https://www.rand.org

https://www.thedefensepost.com/

https://www.defencetalk.com/

https://www.armytimes.com/

AFCEA International
https://www.afcea.org/

Operational AI | Whole of Government Center of Excellence |

William & Mary
https://www.wm.edu/offices/wholeofgovernment/operational-ai/

https://www.airforcetimes.com/

https://www.defense.gov/

http://cyberdefensereview.army.mil

https://spacenews.com/

https://www.army.mil/

https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/

https://www.army-technology.com/

Defense Intelligence Agency(dia.mil)

https://armyrecognition.com/

DIU - Defense Innovation Unit
https://www.diu.mil/

Center for International Maritime Security
https://cimsec.org/

https://www.insaonline.org/

https://thecyberexpress.com/

https://intelligencecommunitynews.com/

US Strategic Command
https://www.stratcom.mil/

Air force Global Strike Command

https://www.afgsc.af.mil/

(InsideDefense.com)
https://insidedefense.com/

Center for European Policy Analysis

https://cepa.org/

CyberUSA
https://www.cyberusa.us/

UNOOSA.ORG

Military Cyber AI

https://militarycyberai.substack.com/

Global Military Grade Cyber Defence Intel Security & AI Analysis – UNDP Soln Exchange | UN Internet Governance Forum | NATO | Information Systems Security Association | National Cybersecurity Alliance | Cloud Security Alliance |
https://easytech4all.net/

https://certinfosec.org

WITH REGARDS TO THE EVOLUTION OF AI INTO AGI

Only under the Leadership and extraordinary imaginative vision of the Worlds Greatest Biological Leaders can AI flourish and evolve into Artificial General Intelligence. Superintelligence through Intelligence Explosion , singularity hypothesis by J . Good's model - " an upgradable intelligent agent could eventually enter a positive feedback loop of self-improvement cycles, each new and more intelligent

generation appearing more and more rapidly, causing a rapid increase ("explosion") in intelligence which would ultimately result in a powerful superintelligence, qualitatively far surpassing all human intelligence ".

Artificial General Intelligence (AGI) is a hypothetical artificial intelligence system that possesses the ability to understand, learn, and apply knowledge across a wide range of tasks, similar to human intelligence. In other words, AGI is a system that can perform any intellectual task that a human can, and possibly more.

The concept of AGI has been debated among experts in the field, and there are different perspectives on what AGI might look like. Here's a simplified breakdown:

Types of AGI:

1. Narrow AGI:A system that can perform a specific task, such as playing chess, solving math problems, or recognizing images.
2. General AGI:A system that can perform any intellectual task that a human can, similar to human intelligence.
3.Superintelligence:A system that can solve complex problems, such as those related to science, philosophy, and ethics.

Characteristics of AGI:

1. Reasoning and problem-solving: AGI systems should be able to reason and solve problems in a way that's similar to

humans.
2. Learning and adaptation:AGI systems should be able to learn from experience and adapt to new situations.
3. Knowledge representation: AGI systems should be able to represent and manipulate knowledge in a way that's similar to humans.
4. Cognitive abilities: AGI systems should be able to simulate human-like cognitive abilities, such as attention, perception, and memory.

Challenges in creating AGI:

1. Scalability: Creating AGI systems that can process and analyze vast amounts of data is a significant challenge.
2. Explainability:AGI systems should be able to explain their decisions and actions, which is a difficult task.
3. Safety and control: AGI systems should be designed to be safe and controllable, which is a complex challenge.

Current research and progress:

While we're still far from creating AGI, researchers are making significant progress in various areas, such as:

1. Deep learning: Techniques like deep learning have shown promise in enabling AGI-like capabilities.
2. Cognitive architectures:Researchers are developing cognitive architectures that can simulate human-like cognitive abilities.
3. Neural networks: Neural networks are being used to

develop AGI-like systems that can learn and adapt.

Challenges and limitations:

1. Current limitations: Currently, AGI systems are limited to specific tasks and don't possess the same level of intelligence as humans.
2. Value alignment: Ensuring that AGI systems align with human values and ethics is a significant challenge.
3.Ethics and governance:Developing frameworks for AGI governance and ethics is essential.

Conclusion:

Artificial General Intelligence is a hypothetical concept that has sparked intense debate and research. While we're making progress in various areas, creating AGI systems that can perform any intellectual task is still a significant challenge. As researchers and experts, we need to continue exploring the possibilities and limitations of AGI to ensure that we're developing systems that can benefit society and humanity as a whole.

Singularity is a complex and multifaceted concept that has been debated and explored by experts in various fields, including artificial intelligence, robotics, neuroscience, and philosophy.

What is a Singularity?

A singularity is a hypothetical event or state in which a

technological or scientific advancement reaches a point where it becomes self-reinforcing, leading to exponential growth in technological advancements, which in turn can lead to a technological singularity. This concept was popularized by mathematician and computer scientist Ray Kurzweil in his book "The Master Plan" (1990) and later by futurist and inventor Ray Kurzweil in his book "The Singularity is Near" (2005).

Types of Singularity

There are several types of singularity that have been proposed:

1. Technological Singularity: A point where a technological advancement becomes self-sustaining, leading to exponential growth in technological advancements.
2. Biological Singularity: A point where a biological process becomes self-sustaining, leading to exponential growth in biological systems.
3. Cognitive Singularity: A point where a cognitive process becomes self-sustaining, leading to exponential growth in cognitive abilities.

Possible Scenarios

There are several possible scenarios that could lead to a singularity:

1. Human Enhancement: Advancements in biotechnology, artificial intelligence, and neuroscience could lead to human

enhancement, where humans can augment their physical and cognitive abilities, potentially leading to a technological singularity.
2. Artificial Intelligence: The development of artificial intelligence could lead to a technological singularity, where AI surpasses human intelligence and becomes self-sustaining.
3. Biotechnology: Advances in biotechnology, could lead to a biological singularity, where biological processes become self-sustaining.
4. Quantum Computing: The development of quantum computing could lead to a technological singularity, where quantum processes become self-sustaining.

Challenges and Concerns :

While the concept of a singularity is intriguing, there are many challenges and concerns associated with it:

1. Unintended Consequences: A singularity could lead to unintended consequences, such as the loss of human agency, the degradation of the environment, or the emergence of a new form of life that is incompatible with human society.
2. Ethical and Moral Implications: A singularity raises important ethical and moral questions, such as the potential for a new form of life to be created, the potential for human enhancement to be misused, and the potential for the loss of human dignity.
3. Uncertainty and Complexity: The concept of a singularity is inherently uncertain and complex, making it difficult to predict and prepare for the potential consequences of such an event.

In conclusion, the concept of a singularity is a complex and multifaceted idea that raises important questions and challenges. While it's impossible to predict the outcome of a singularity, it's essential to consider the potential risks and benefits associated with such an event.

The Hungarian-American mathematician John von Neumann (1903-1957) became the first known person to use the concept of a "singularity" in the technological context.Stanislaw Ulam reported in 1958 an earlier discussion with von Neumann "centered on the accelerating progress of technology and changes in the mode of human

life, which gives the appearance of approaching some essential singularity in the history of the race beyond which human affairs, as we know them, could not continue".Subsequent authors have echoed this viewpoint.

The concept and the term "singularity" were popularized by Vernor Vinge - first in 1983 (in an article that claimed that once humans create intelligences greater than their own, there will be a technological and social transition similar in some sense to "the knotted space-time at the center of a black hole", and later in his 1993 essay The Coming Technological Singularity, (in which he wrote that it would signal the end of the human era, as the new superintelligence would continue to upgrade itself and would advance technologically at an incomprehensible rate). He wrote that he would be surprised if it occurred before 2005 or after 2030.Another significant contributor to wider circulation of the notion was Ray Kurzweil's 2005 book The Singularity Is

Near, predicting singularity by 2045.

Landmark resolution on AI by UN General Assembly on 21st March 2024 – Global Military Grade Cyber Defence Intel Security & AI Analysis

https://easytech4all.net/2024/03/26/landmark-resolution-on-ai-by-un-general-assembly-on-21st-march-2024/

Cyber Stability Conference 2025 UNIDIR

https://unidir.org/event/cyber-stability-conference-2025/

Outer Space Security Conference 2025 UNIDIR

https://unidir.org/event/outer-space-security-conference-2025/

Agenda & Events | Geneva Cyber Week 2025

https://genevacyberweek.com/en/agenda-and-events

From words to protection – how do cyber norms guide security of critical infrastructure? Announcing Chapter II of the Geneva Manual – Geneva Dialogue

https://genevadialogue.ch/event/announcing-second-chapter/

Artificial Intelligence - Global Landscape

About – Global Military Grade Cyber Defence Intel Security & AI Analysis by GROK

https://easytech4all.net/about/

About - Military Cyber AI by GROK

https://militarycyberai.substack.com/about

Militarised Cyber AI (Aggregate Archives)

https://militarycyberai.substack.com/p/militarised-cyber-ai-aggregate-archives

Biological Encephalon vs Artificial Neural Networks (GROK analysis)

https://militarycyberai.substack.com/p/biological-encephalon-vs-artificial

Recent Updates :

Ran some tests through Meta AI , Google Gemini , ChatGPT , Anthrophic Claude Sonnet and Brave Leo AI for simplification of Military and Cyber Space Defense Intelligence Strategic Analysis at easytech4all.net

https://easytech4all.net/2025/04/12/ran-some-tests-through-meta-ai-google-gemini-chatgpt-anthrophic-claude-sonnet-and-brave-leo-ai-for-simplification-of-military-and-cyber-space-defense-intelligence-strategic-analysis-at-eas/

Evaluated Easytech4all.net through the eyes of Google Gemini , Open AI ChatGpt , Brave Leo AI , Anthorpic Claude , Meta AI – Global Military Grade Cyber Defence Intel Security & AI Analysis

https://easytech4all.net/2025/04/28/evaluated-easytech4all-net-through-the-eyes-of-google-gemini-open-ai-chatgpt-brave-leo-ai-anthorpic-claude-meta-ai/

OpenAI’s Chatgpt Evaluates Military Defense Grade Blogging / Website – Global Military Grade Cyber Defence Intel Security & AI Analysis

https://easytech4all.net/2025/01/05/openais-chatgpt-evaluates-military-defense-grade-blogging-website/

Global Military Grade Cyber Defence Intel Security & AI Analysis – UNDP Soln Exchange | UN Internet Governance Forum | NATO | Information Systems Security Association | National Cybersecurity Alliance | Cloud Security Alliance |

https://easytech4all.net/

Integrated All Domain Warfare | Militarised AI and CyberNet | Global Strategic Analysis – Global Military Grade Cyber Defence Intel Security & AI Analysis

https://easytech4all.net/2025/03/21/integrated-all-domain-warfare-militarised-ai-and-cybernet-global-strategic-analysis/

Top 100 Military Defense Companies – Global Military Grade Cyber Defence Intel Security & AI Analysis

https://easytech4all.net/2024/09/01/top-100-military-defense-companies/

CyberAI-CyberAGI(Projection) – Global Military Intelligence Industrial Defense Complex. – Global Military Grade Cyber Defence Intel Security & AI Analysis

https://easytech4all.net/2024/01/17/cyberai-cyberagiprojection-global-military-intelligence-industrial-defense-complex/

United States Air Force Militarised Android Tactical Awareness Kit. – Global Military Grade Cyber Defence Intel Security & AI Analysis

https://easytech4all.net/2025/02/12/united-states-air-force-militarised-android-tactical-awareness-kit/

USAV 2025 – Global Military Grade Cyber Defence Intel Security & AI Analysis

https://easytech4all.net/2025/03/06/usav-2025/

Global Cyber Intelligence by Military and Intelligence Agencies way ahead of our times in true sense of the term – Global Military Grade Cyber Defence Intel Security & AI Analysis

https://easytech4all.net/2024/11/09/global-cyber-intelligence-by-military-and-intelligence-agencies-way-ahead-of-our-times-in-true-sense-of-the-term/

US perplexity AI Analyzes military Cyber ai Defence platform

https://easytech4all.net/2025/04/05/us-perplexity-ai-analyzes-military-cyber-ai-defense-rational-cerebration/

Military Grade Cyber Defense Intelligence AI review

https://easytech4all.net/2025/01/02/global-military-grade-cyber-defense-intelligence-and-ai-review-2024/

2024 in Review - Military | Defense | Cyber | AI | Space | Nuclear

https://easytech4all.net/2024/12/28/2024-in-review-attitude-

of-gratitude/

How algorithmocracy secures the astounding arenas of Military , Cyberelectronic Space and Nuclear ? Brief evaluation of the Point of Inception for origin extraction and determination. Human Generated Analysis follows

https://easytech4all.net/2024/12/08/algorithmocracy-global-military-machine-cyberai-space-nuclear-energy/

Abstract Detailing semantics of hypothetical Global Cyber Incident and autonomous Military Grade Cyber Defense.

https://easytech4all.net/2024/11/15/abstract-detailing-semantics-of-hypothetical-cyber-incident-and-autonomous-military-grade-cyber-defense-system/

CIA Triad and Defense in Depth Strategy

https://easytech4all.net/2024/11/09/notes-on-cia-triad-model-and-defense-in-depth-strategy/

Upskilling and Essential Deliberations.

https://easytech4all.net/2024/10/14/upskilling-essential-deliberations-cybersecurity-awareness-month/

Arrow of time Intelligence and orphic Dimensions.

https://easytech4all.net/2024/09/28/the-arrow-of-time-intelligence-orphic-dimensions/

AI Global Strategic Information modelling Analysis

https://easytech4all.net/2024/09/17/ai-and-global-strategic-information-modelling-analysis/

Qatar’s AI strategy

https://easytech4all.net/2024/09/14/qatars-aix-future-levitating-towards-the-arc-of-artificial-general-intelligence/

AI global Security and military Grade open source intelligence

https://easytech4all.net/2024/07/26/ai-global-security-

military-grade-open-source-intelligence/

Global Cyber Intelligence Analytics and large language Models.

https://easytech4all.net/2024/07/12/global-cyber-intelligence-analytics-ai-large-learning-language-model-training-youtube/

Some Global Military Cyber AI defense reports and presentations

https://easytech4all.net/2024/05/21/some-reports-and-1000-

slide-presentations-on-ai-and-global-cyber-intelligence/

The US Department of Defense - Pentagon - Global Military Defense.

https://easytech4all.net/2024/06/23/they-call-you-the-1/

AI and US Bombers.

https://easytech4all.net/2024/05/04/ai-and-the-us-b-24-liberator-strategic-stealth-bomber/

Autonomous Cyber Defense , Cyber Networks and Nuclear Systems.

https://easytech4all.net/2024/04/20/autonomous-cyber-defense-militarised-cyber-networks-nuclear-systems-security/

Exploratory analysis of variance in Quest for sympathizing with CyberAI for efficacious Military /Defense Cyberspace Intelligence penning . ' Intriguing perspective by the practitioners of Military Writing on Doctrines etc...

https://easytech4all.net/2024/04/07/decussation-of-military-defense-cyberspace-intelligence-analysis-with-respect-to-data-info-ingestion-for-ai-ml-large-language-models/

Landmark Resolution on AI by UN General Assembly

https://easytech4all.net/2024/03/26/landmark-resolution-on-

ai-by-un-general-assembly-on-21st-march-2024/

Cyber Intelligence Command Center of a Global Military Alliance Headquarters somewhere in the Northern Hemisphere.

https://easytech4all.net/2024/03/20/after-hours-conversations-between-binary-digits-0-and-1-at-the-cyber-intelligence-command-center-of-a-global-military-alliance-hq-somewhere-in-the-northern-hemisphere/

Random Simulation in a conjectural multidimensional visual world ofcourse augmented by the powerful super computers (AURORA AT ARGONNE) or maybe quantum computers (by D - Waves)

https://easytech4all.net/2024/03/10/3929/

CYber AI and the Ostensible intergalactic Cyber Electronic Portal Landscape - Through the Lens of Hyper Visions as if powered by real world hypervisors.

https://easytech4all.net/2024/03/04/cyber-ai-ostensible-intergalactic-cyber-electronic-portal-military-and-cyber-commands/

AI Cybersecurity & Advanced Cyber Defense IntelligenceMilitarisation of the Origins and present of Modern Day State of ArtDisruptive Technology.Notes , Blog Archives , Weblinks , ReferencesObservations , Research & Analysis.Mind…

https://easytech4all.net/2024/01/31/global-cyber-defense-intelligence-document-vol-2/

Cybersecurity , Advanced Cyber Threat Intelligence and Artificial Intelligence Rationale and Paradigms .Some Notes , Mind Maps , Infographics, Observations, Research and Analysis , CyberAI Blog Archives and web links…

https://easytech4all.net/2023/12/23/cyber-intelligence-and-cyberai-research-analysis-document-update-dec-2023/

At the intersection of Cyber AI and Cyber Intelligence

https://easytech4all.net/2023/12/21/at-the-intersection-of-cyberai-and-cyber-threat-intelligence/

Precognitive AI

https://easytech4all.net/2023/12/21/precognitive-ai-clairvoyant-or-appurtenant-invention-or-discovery/

DIY's Instructubles and Self Help Guides . Learning Resources Archives for Generative AI , Distributed Advanced Cyber Threat Intelligence, Open Source Software and OS Security , Quantum and Decentralised Meshnetworking

https://easytech4all.net/2023/11/27/ai-and-cyber-defense-beginner-to-advanced-intelligence-resources-and-analysis/

Cyberspace Origins and frontier AI

https://easytech4all.net/2023/11/25/cyberspace-origins-and-frontier-ai/

CyberAI transforms Cyber Intelligence

https://easytech4all.net/2023/11/16/cyberai-transubstantiates-cyber-threat-intelligence/

GenAI Disinformation Mitigation Strategies and Global Competition. Highlighted the dangers of Dis/Mis information and Deepfakes - NATO | USDOD | Government of Germany

Recap of Advanced Cyber Threat Intelligence Paradigms & Countermeasures

https://easytech4all.net/2023/10/21/the-inevitability-of-militarisation-of-cyberai/

7th Annual Defense News Conference.

https://easytech4all.net/2023/09/11/7th-annual-defense-news-conference/

Controlling and owning the battlespace of today and tomorrow requires theability to observe, orient, decide, and act on trusted and validated information at the speed of relevance.

https://easytech4all.net/2024/02/09/google-defense-forum/

Advanced Cyber Threat Intelligence Document and Presentation (Notes , MindMaps , Infographics , Webinars , Research and Analysis , Brainstorms etc) with Global Cyber Intelligence Organisations , Millitary Alliances…

https://easytech4all.net/2023/08/30/advanced-cyber-threat-intelligence-document-presentation/

Q&A with Google Bard (Now Google Gemini)

https://easytech4all.net/2023/08/30/my-qa-sessions-with-google-bard-large-language-model-a-little-organised-readers-discretion-advised/

Interactions with OpenAI’s ChatGpt

https://easytech4all.net/2023/08/28/some-interactions-with-openais-chatgpt4-on-ai-and-relevant-domains-readers-discretion-advised/

My Interactions with Google's Bard on Post Quantum Cryptography , Quantum Super Computing , large scale distributed decentralised Mesh Computing (Application in AI) , JADC2 and Global Information Dominance Experiments,…

https://easytech4all.net/2023/08/28/rendezvous-with-googles-bard-beta/

Google Cloud Security

https://easytech4all.net/2023/06/07/google-cloud-security-2023/

Cyber Power At the heart of a Nation States strategy is theconcept of cyber power, which is defined as the ability of a state to protect and promote its interests

https://easytech4all.net/2023/06/07/3669/

Global Cyber Intelligence consecrated

https://easytech4all.net/2023/06/07/global-cyber-intelligence-consecrated/

2023 Cyber Stability Conference - Use Of ICTs By States: Rights And Responsibilities Under The UN Charter .The United Nations Institute for Disarmament Research (UNIDIR)

https://easytech4all.net/2023/04/02/unidir-cyber-stability-conference-2023/

Cyber Attack Vectors What is Zero Trust Network Access Zero Trust Network Access Software Defined Perimeter Zero Trust Implementation by DOD and Cyber Command Quick CT landscape Pentagons Zero Trust...

https://easytech4all.net/2023/03/21/quick-global-cyber-threat-intelligence-observations-22-23/

2021 Cyber Stability Conference: Towards A More Secure

Cyberspace Over the past two decades, Member States' discussions have focused on the use of information and communications technologies

https://easytech4all.net/2022/07/05/unidir-cyber-stability-conference-3rd-december-friday-2021/

U.S. Cyberspace Solarium Commission Webinar:Accomplishments and Next Steps for U.S. Cyber Policy

https://easytech4all.net/2022/04/10/us-cyberspace-solarium-commission/

Safe and Secure Digital Ecosystems for students.

https://easytech4all.net/2022/04/10/safe-and-secure-digital-ecosystems-for-students/

UN Security Council Cyber Threats Debate

https://easytech4all.net/2022/03/06/un-security-council-cyberthreats-debate/

Military and Space - Strategic Competition

https://easytech4all.net/2022/03/06/threats-to-satellite-navigation-system-conflict-in-space/

Cyber Intelligence Unit

https://easytech4all.net/2022/02/24/cyber-intelligence-unit-ciu-q4-2021/

Annual Cybersecurity Summit by US CISA

https://easytech4all.net/2022/02/07/4th-annual-national-cybersecurity-summit-by-cisa/

Cyber Defence Threat Intelligence talks

https://easytech4all.net/2022/02/05/cyber-defense-threat-intelligence-talks/

UNIDIR - INFORMATION AND COMMUNICATION TECHNOLOGIES

https://easytech4all.net/2022/02/05/unidir-ict-information-communication-technologies/

Cyber Attack and Aviation Sector

https://easytech4all.net/2022/02/05/cyberattack-and-aviation-sector/

Cyber Polygon 2020 , 2021 and Upcoming 2022 - This project is part of the World Economic Forum’s Centre for Cybersecurity Platform and INTERPOL .

https://easytech4all.net/2022/01/16/cyber-

polygon-2020-2021-and-2022/

Zero trust architecture and advanced cyber threat intelligence

https://easytech4all.net/2021/10/10/zero-trust-architectured-networks-advanced-cyber-threat-intelligence/

National Cybersecurity Awareness Month

https://easytech4all.net/2021/10/10/national-cybersecurity-awareness-month-ncam-advanced-cyber-threat-intelligence/

https://easytech4all.net/2021/10/10/national-cybersecurity-awareness-month-ncam-critical-infrastructure/

Cyber Threat Intelligence in Military Defense

https://easytech4all.net/2021/10/10/cyber-threat-intelligence-in-defense/

Cyber Risk - Recorded Future.

https://easytech4all.net/2021/10/10/cyber-risk-is-everywhere-in-a-nutshell/

Advanced Cyber Intelligence Livestream

https://easytech4all.net/2021/10/06/advanced-cyber-threat-intelligence-1-hr-livestream-recording/

Cyber Intelligence Documentary

https://easytech4all.net/2021/10/06/cyber-threat-intelligence-documentary/

Cyber Threat Intelligence Content Management systems.

https://easytech4all.net/2021/10/06/watch-cyber-threat-intelligence-cms-research-analysis-on-youtube/

Global Cyber Threat Landscape 2021

https://easytech4all.net/2021/10/06/global-cyber-threat-landscape-2021/

Global Cyber Threats Operating System Solutions

https://easytech4all.net/2021/10/06/global-cyber-threats-mobile-os-soutions/

Challenges faced by Law Enforcement

https://easytech4all.net/2021/10/06/watch-challenges-faced-by-govt-and-int-law-enforcement-cybersec-on-youtube/

US - Dept of Homeland Security - Cyber Threat is Real

https://easytech4all.net/2021/10/01/the-cyberthreat-is-real-

us-dhs/

https://easytech4all.net/2021/10/01/cyber-essentials-by-us-dhs/

US FBI - Ransomware

https://easytech4all.net/2021/10/01/ransomware-fbis-perspective/

Goldmine for exchanging Cyber Threat Intelligence

https://easytech4all.net/2021/10/01/global-study-on-exchanging-cyber-threat-intelligence/

US FBI | CISA | DHS | CID - Countering Ransomware

https://easytech4all.net/2021/10/01/countering-ransomware-attacks-fbi-cisa-dhs-cid/

Strategic Threat Hunting

https://easytech4all.net/2021/10/01/strategic-threat-hunting-advanced-cyber-threat-intelligence/

Cyber Intelligence Paradigms

https://easytech4all.net/2021/10/01/cybersec-cyber-threat-intelligence-paradigms/

Cyberspace and Cyber Warfare Threat Intel assessment

https://easytech4all.net/2021/10/01/cyberspace-flashpoint-cyber-warfare-threat-intelligence-assessment/

World War 3 and Cyberspace insights

https://easytech4all.net/2021/10/01/ww3-cyberspace-insights/

Cyber Kinetic War - Birds eye view

https://easytech4all.net/2021/10/01/cyber-warfare-advanced-cyber-threat-intelligence-assessment/

https://easytech4all.net/2021/10/01/cyber-threat-landscape-birds-eye-view/

Cyberattacks and critical infrastructure

https://easytech4all.net/2021/10/01/cyberattacks-critical-infrastructure-nato/

Quintessence Kingdoms and Light – Global Cyber Defence Intelligence | Strategic Communications – CyberSpace AI | OS Hardening | Adv Integrated Modular Battlefield Management System | Research & Analysis

https://easytech4all.net/2024/09/12/quintessence-kingdoms-and-light/

AI and Global Strategic Information Modelling Analysis –

Global Cyber Defence Intelligence | Strategic Communications – CyberSpace AI | OS Hardening | Adv Integrated Modular Battlefield Management System | Research & Analysis

https://easytech4all.net/2024/09/17/ai-and-global-strategic-information-modelling-analysis/

Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations – Global Military Grade Cyber Defence Intel Security & AI Analysis

https://easytech4all.net/2020/12/24/advanced-persistent-threat-compromise-of-government-agencies-critical-infrastructure-and-private-sector-organizations/

Biggest CyberAttack on World's Leading CyberPower. – Global Military Grade Cyber Defence Intel Security & AI Analysis

https://easytech4all.net/2020/12/24/biggest-cyberattack-on-worlds-leading-cyberpower/

Now+Next : Countering Ransomware Attacks. – Global Military Grade Cyber Defence Intel Security & AI Analysis

https://easytech4all.net/2021/05/09/nownext-countering-ransomware-attacks/

Global Accreditation Webinars & brainstorming for Advanced Cyber Defense Threat Intelligence – Global Military Grade Cyber Defence Intel Security & AI Analysis

https://easytech4all.net/2021/01/19/global-accreditation-webinars-brainstorming-for-advanced-cyber-defense-threat-intelligence/

Global Internet Ranking for Advanced Cyber Threat Intelligence – Global Military Grade Cyber Defence Intel Security & AI Analysis

https://easytech4all.net/2020/12/28/global-internet-ranking-for-advanced-cyber-threat-intelligence/

CyberAI – Global Strategic Imperative – Global Military Grade Cyber Defence Intel Security & AI Analysis

https://easytech4all.net/2023/06/07/3669/

Countering Ransomware Attacks | FBI CISA DHS CID – Global Military Grade Cyber Defence Intel Security & AI Analysis

https://easytech4all.net/2021/10/01/countering-ransomware-attacks-fbi-cisa-dhs-cid/

7th Annual Defense News Conference – Global Military Grade Cyber Defence Intel Security & AI Analysis

https://easytech4all.net/2023/09/11/7th-annual-defense-news-conference/

State of American Business 2023 – Global Military Grade Cyber Defence Intel Security & AI Analysis

https://easytech4all.net/state-of-american-business-2023/

US Chamber Cyber Conference with US Federal Security Agencies – Global Military Grade Cyber Defence Intel Security & AI Analysis

https://easytech4all.net/cyber-conference/

Intelligence and National Security Alliance 2024 (UPDATE) – Global Military Grade Cyber Defence Intel Security & AI Analysis

https://easytech4all.net/future-of-intelligence-community-workforce/

1 Power Cybersec CTI Brainstorms – Global Military Grade Cyber Defence Intel Security & AI Analysis

https://easytech4all.net/1-power-cybersec-cti-brainstorms/

UK Cybersecurity Association | 1 day Summit – Global Military Grade Cyber Defence Intel Security & AI Analysis

https://easytech4all.net/uk-cybersecurity-association-1-day-summit/

UN IGF Solution Exchange – Global Military Grade Cyber Defence Intel Security & AI Analysis

https://easytech4all.net/un-igf-solution-exchange/

7th Annual Defense News Conference – Global Military Grade Cyber Defence Intel Security & AI Analysis

https://easytech4all.net/2023/09/11/7th-annual-defense-news-conference/

GLOBAL ANALYSIS , REPORTS , ARTICLES , WHITEPAPERS , RESEARCH - AI and AGI

USA

OpenAI: Announcing The Stargate Project

https://openai.com/index/announcing-the-stargate-project/

The New York Times: Trump Announces $100 Billion Stargate A.I. Initiative With OpenAI, Oracle and SoftBank

https://www.nytimes.com/2025/01/21/technology/trump-

openai-stargate-artificial-intelligence.html

GeekWire: Microsoft and OpenAI tweak the terms of their cloud deal, enabling $500B Stargate AI project

https://www.geekwire.com/2025/microsoft-and-openai-tweak-the-terms-of-their-cloud-deal-enabling-500b-stargate-ai-project/

Trump announces a $500 billion AI infrastructure investment in the US | CNN Business

Trump announces a $500 billion AI infrastructure investment in the US | CNN Business

https://amp-cnn-com.cdn.ampproject.org/v/s/amp.cnn.com/cnn/2025/01/21/tech/openai-oracle-softbank-trump-ai-investment?amp_js_v=0.1&amp_gsa=1#webview=1

Engadget: NVIDIA is going to make AI chips and supercomputers in the US

https://www.engadget.com/computing/nvidia-is-going-to-make-ai-chips-and-supercomputers-in-the-us-213534618.html

Ars Technica: Google’s Gemma 3 is an open source, single-GPU AI with a 128K context window

https://arstechnica.com/gadgets/2025/03/googles-new-

gemma-3-ai-model-is-optimized-to-run-on-a-single-gpu/

The Verge: Google calls Gemma 3 the most powerful AI model you can run on one GPU

https://www.theverge.com/ai-artificial-intelligence/627968/google-gemma-3-open-ai-model

Google DeepMind: Gemini Robotics brings AI into the physical world

https://deepmind.google/discover/blog/gemini-robotics-brings-ai-into-the-physical-world/

AI at Meta: The Llama 4 herd: The beginning of a new era of natively multimodal AI innovation

https://ai.meta.com/blog/llama-4-multimodal-intelligence/

The Washington Post: Elon Musk says his AI company and X are merging

https://www.washingtonpost.com/technology/2025/03/28/xai-acquires-x-elon-musk/

United States Air Force Militarised Android Tactical Awareness Kit. – Global Military Grade Cyber Defence Intel Security & AI Analysis

https://easytech4all.net/2025/02/12/united-states-air-force-militarised-android-tactical-awareness-kit/

A trillion-dollar defense budget? | Defense News Weekly Full Episode

https://www.defensenews.com/video/2025/04/25/a-trillion-dollar-defense-budget-defense-news-weekly-full-episode-42625/

Inside Project Maven, the US Military's Mysterious AI Project | Big Take - YouTube

https://m.youtube.com/watch?v=E1OQwTCkIIA

Pentagon signs AI deal to aid military decision-making

https://thehill.com/policy/technology/5178088-pentagon-signs-ai-deal-to-aid-military-decision-making/amp/

Pentagon Selects Scale AI to Support AI-Driven Military Planning, Decision-Making

https://thedefensepost.com/2025/03/06/pentagon-ai-military-planning/amp/

Pentagon to build AI for war planning in Europe and Asia - Defense One

https://www.defenseone.com/technology/2025/03/

pentagon-build-ai-war-planning-europe-and-asia/403506/

AI for war plans: Pentagon innovation shop taps Scale AI to build 'Thunderforge' prototype - Breaking Defense

http://breakingdefense.com/2025/03/ai-for-war-plans-pentagon-innovation-shop-taps-scale-ai-to-build-thunderforge-prototype/

Pentagon to build AI for war planning in Europe and Asia - Defense One

https://www.defenseone.com/technology/2025/03/pentagon-build-ai-war-planning-europe-and-asia/403506/

Pentagon contract ‘Thunderforge’ will make AI tools for military planning - The Washington Post

https://www.washingtonpost.com/technology/2025/03/05/pentagon-ai-military-scale/

United States’ Project Maven And The Rise Of AI-Assisted Warfare — Global Defense Insight

https://defensetalks.com/united-states-project-maven-and-the-rise-of-ai-assisted-warfare/

Palantir wins contract to expand access to Project Maven AI tools

https://www.c4isrnet.com/artificial-intelligence/2024/05/30/palantir-wins-contract-to-expand-access-to-project-maven-ai-tools/

Fact Sheet: President Donald J. Trump Advances AI

Education for American Youth – The White House

https://www.whitehouse.gov/fact-sheets/2025/04/fact-sheet-president-donald-j-trump-advances-ai-education-for-american-youth/#:~:text=The%20task%20force%20will%20plan,philanthropy%2C%20and%20industry%20to%20address

Advancing Artificial Intelligence Education for American Youth – The White House

https://www.whitehouse.gov/presidential-actions/2025/04/advancing-artificial-intelligence-education-for-american-youth/

Shield AI acquires post-mission analysis tool to strengthen its autonomy systems

https://www.janes.com/osint-insights/defence-news-details/air/shield-ai-acquires-post-mission-analysis-tool-to-strengthen-its-autonomy-systems

National Security in the Digital Age: Leveraging America's Technical Advantage - Two Six Technologies

https://twosixtech.com/resources/white-paper/national-security-in-the-digital-age-leveraging-americas-technical-advantage-insa/

An Experiment: Eighth Army Operational Effects Directorate

https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2025/Eighth-Army-Experiment/

US DOD Scientific Research and Innovation

https://www.linkedin.com/posts/deptofdefense_scientific-research-innovations-activity-7321231481232625666-D8Wb?utm_source=share&utm_medium=member_android&rcm=ACoAACRUtIMBLE8oKip-rtyqKnAIcBikjnTMWYY

TechCrunch: Exclusive: Earth AI’s algorithms found critical minerals in places everyone else ignored

https://techcrunch.com/2025/03/25/earth-ais-algorithms-found-critical-minerals-in-places-everyone-else-ignored/

Scale AI’s Huge DoD Deal

https://youtu.be/iSpEH_1rf0M?si=9QJ3I_89IMEbXPQI

AI is expected to add over $4 trillion to the global economy. Here's how data centres can handle AI's power consumption sustainably.

https://www.weforum.org/stories/2025/01/the-essential-energy-shift-for-sustainable-genai/?utm_source=whatsapp&utm_medium=social

UK and Europe

NATO picks Palantir's Maven AI for military planning, amid trans-Atlantic tension - Breaking Defense

https://breakingdefense.com/2025/04/nato-picks-palantirs-maven-ai-for-military-planning-amid-trans-atlantic-tension/

TechCrunch: Macron unveils $112B AI investment package,

https://techcrunch.com/2025/02/10/macron-unveils-a-112b-ai-investment-package-as-frances-answer-to-stargate/

How is Europe becoming a leader in AI?

https://youtu.be/i268oenkv0U?si=iiFp0-ScPeUYidwh

Al Arabiya English: Saudi Arabia, Italy ink $10 billion cooperation and industrial deals

https://english.alarabiya.net/News/saudi-arabia/2025/01/26/italian-prime-minister-giorgia-meloni-arrives-in-saudi-arabia-

POLITICO Europe: How the world stopped worrying and

learned to love AI

https://www.politico.eu/article/ai-action-summit-france-paris-macron-vance-modi-artificial-intelligence-technology/

Royal United Services Institute: Quantum Technologies in the UK

https://www.rusi.org/news-and-comment/explainers/quantum-technologies-uk

GOV.UK: £121 million boost for quantum technology set to tackle fraud, prevent money laundering and drive growth

https://www.gov.uk/government/news/121-million-boost-for-quantum-technology-set-to-tackle-fraud-prevent-money-laundering-and-drive-growth

Prime Minister sets out blueprint to turbocharge AI - GOV.UK

Reuters UK: Prime Minister Starmer plans to make Britain AI 'superpower'

https://www.reuters.com/world/uk/uk-pm-starmer-outline-plan-make-britain-world-leader-ai-2025-01-12/

Case study: The University of Greenwich - NCSC.GOV.UK

https://www.ncsc.gov.uk/case-study/the-university-of-greenwich

Prime Minister Starmer plans to make Britain AI 'superpower' | Reuters

https://www.reuters.com/world/uk/uk-pm-starmer-outline-plan-make-britain-world-leader-ai-2025-01-12/

Prime Minister sets out blueprint to turbocharge AI - GOV.UK

https://www.gov.uk/government/news/prime-minister-sets-out-blueprint-to-turbocharge-ai

Too Good to Be True? Understanding the Risks of Free OSINT Tools

https://www.osint.uk/content/too-good-to-be-true-understanding-the-risks-of-free-osint-tools

Macron unveils $112.5 bn AI investment to boost France's tech ambitions | World News - Business Standard

https://www.google.com/amp/s/www.business-standard.com/amp/world-news/french-president-emmanuel-macron-ai-data-centre-stargate-donald-trump-eu-125021000838_1.html

France's AI Summit: Private Sector Plans to Invest $112 Billion

https://variety.com/2025/digital/global/france-ai-summit-

private-sector-112-billion-1236302473/

NATO acquires AI-enabled Warfighting System

https://shape.nato.int/news-releases/nato-acquires-aienabled-warfighting-system-
https://www.gov.uk/government/news/prime-minister-sets-out-blueprint-to-turbocharge-ai

NATO picks Palantir’s Maven AI for military planning, American Combatant Commands worldwide already make heavy use of Palantir’s Maven Smart System to rapidly share and analyze planning data. Now NATO will start using it too.

https://info.breakingdefense.com/e3t/Ctc/GA+113/cfk9804/MVWLJvgkCLqW1bkX4j721_ySW5JQdxX5vNbM2N2L_pyH5nR32W5BWr2F6lZ3pZVbs7qZ6h0jbKW97fS1r7RV6wZW43wDlz8ZycSQN26rjkbd-h1DW2wSv_97vx3TYW51nZPB1ltH4yW6Kr9Q15rVtK9W2Kf-QZ6f19G-W6TbNsl7jvQbNW1JBrD18j54zDW5-nFGf3sm4dfW2DyHKz3g8bT9W5dnNbQ8JTLy6W93ncCl87qtf1W45KzV-2vBXQfW7qmcH12Zb_NGW26R-KT8St7ZHW5Jb7_k8HNcyHMBbhpR481zyW8WbKd-54p0_5N56QCm4dMnS8VWTSZ83mH0gSW3bMJVf73t4XgW1rwlMd24rCxjW7CBTqN3BrfhRW91mJMG6mlSXdV4ccYw57Dcs-W1fRljT276trKW6RHr5J4r_6lxW698s1s1M5NT9W1VqVQn1R8s0SVZ6jVr462QTKW5hkF7T2vK1StW73L5rH6zWqTpf67NFyl

04

Microsoft: Innovating in line with the European Union’s AI Act

https://blogs.microsoft.com/on-the-issues/2025/01/15/innovating-in-line-with-the-european-unions-ai-act/

Henry Kissinger and Graham Allison, “The Path to AI Arms Control,” Foreign Affairs, October 13, 2023, https://www.foreignaffairs.com/united-states/henry-kissinger-path-artificial-intelligence-arms-control.

The race for artificial intelligence - Can Europe compete? | DW Documentary

https://youtu.be/i8ljZYzn0Uc

Gulf Cooperation Council (MENA - Middle East North Africa)

AIM: Saudi Arabia Eyes $12.8 Bn to Build Data Centre

https://analyticsindiamag.com/ai-news-updates/saudi-arabia-eyes-12-8-bn-to-build-data-centre/

A pioneering researcher shares why he’s so optimistic about AI:

https://restofworld.org/2025/juergen-schmidhuber-ai-saudi-arabia-tech/

Arab News: Crown prince to Trump: Saudi Arabia seeks to push US investments to $600bn during second term

https://www.arabnews.com/node/2587456/saudi-arabia

National Cyber Security Strategy 2024-2030 launched | The Peninsula Qatar
https://m.thepeninsulaqatar.com/article/18/09/2024/national-cyber-security-strategy-2024-2030-launched

Qatar’s initiatives on digital skills attracts dynamic workforce | The Peninsula Qatar
https://m.thepeninsulaqatar.com/article/18/09/2024/qatars-initiatives-on-digital-skills-attracts-dynamic-workforce

Ask Ai.SHA: Invest Qatar announces launch of new chatbot initiative - Doha News | Qatar
https://dohanews.co/ask-ai-sha-invest-qatar-announces-launch-of-new-chatbot-initiative/

Invest Qatar launches Ai.SHA, an Azure Open AI GPT-powered chatbot
https://www.invest.qa/en/media-and-events/news-and-articles/invest-qatar-launches-aisha-an-azure-open-ai-gpt-powered-chatbot

An AI-Enabled Future for Qatar and the Region – Communications of the ACM
https://cacm.acm.org/research/an-ai-enabled-future-for-qatar-and-the-region/

Inside Qatar's AI project that aims to preserve the Arabic language | WIRED Middle East
https://wired.me/technology/ai-preserve-arabic-language/

Qatar is leading the world in AI; here's how – Middle East & Africa News Center
https://news.microsoft.com/en-xm/2023/12/19/qatar-is-leading-the-world-in-ai-heres-how/

'Qatar aims to lead in global AI race' | The Peninsula Qatar
https://m.thepeninsulaqatar.com/article/05/06/2024/qatar-aims-to-lead-in-global-ai-race

Qatar's startup ecosystem jumps 11 places in global index | The Peninsula Qatar
https://m.thepeninsulaqatar.com/article/08/09/2024/qatars-startup-ecosystem-jumps-11-places-in-global-index

Qatar to Invest Billions of Dollars in AI, PM Says

https://youtu.be/MfvTkFY7Dbg?si=u_48UxJt_G90CpTi

UAE

UAE, US agree on $1.4 trillion in investments over 10 years, White House says - Aletihad News Center
https://en.aletihad.ae/news/uae/4561070/uae--us-agree-on--1-4-trillion-in-investments-over-10-years

Hamdan bin Mohammed: AI is the cornerstone in designing Dubai’s future

https://www.emirates247.com/technology/hamdan-bin-mohammed-ai-is-the-cornerstone-in-designing-dubai-s-future-2025-04-20-1.738775

UAE AI Minister Omar Al Olama on the era of artificial intelligence

https://www.youtube.com/live/3SwOCTaO4IM?si=W_2T9qL4gg5qBwuz

UAE, US agree on $1.4 trillion in investments over 10 years, White House says

http://link.aletihad.ae/J8Xe

http://link.aletihad.ae/J8Xe

The potential of AI-driven business solutions on the SME industry .

https://www.youtube.com/live/gHRNv09TyP0?si=g6Ffi9iiN4iSXUZP

e& UAE revolutionises telecom tower inspections with AI-powered drones

https://wam.ae/a/bj7h60w

National cybersecurity systems respond to cyberattacks targeting government, private entities

https://www.wam.ae/a/bits7qz

Mohammed bin Rashid meets with core team behind successful hosting of World Governments Summit 2025

https://x.com/WAMNEWS_ENG/status/1890117294707335471

Hamdan bin Mohammed attends graduation ceremony of Arab, global leadership, capacity-building programmes

https://x.com/WAMNEWS_ENG/status/1890107826883957116

UAE, French Presidents discuss bilateral ties in Paris, witness signing of UAE-France Framework for Cooperation in Artificial Intelligence

https://www.wam.ae/a/15ep5zv

Dubai AI Week Expands Agenda with Global Events Focused on Education and Health

https://www.emirates247.com/technology/dubai-ai-week-expands-agenda-with-global-events-focused-on-education-and-health-2025-04-18-1.738758

Mohammed bin Rashid honours graduates of the Federal Artificial Intelligence Programme

https://www.emirates247.com/uae/mohammed-bin-rashid-honours-graduates-of-the-federal-artificial-intelligence-programme-2025-04-16-1.738714

UAE Cabinet, chaired by Mohammed bin Rashid, approves launch of first integrated regulatory intelligence ecosystem in UAE Government

https://www.emirates247.com/uae/uae-cabinet-chaired-by-mohammed-bin-rashid-approves-launch-of-first-integrated-regulatory-intelligence-ecosystem-in-uae-government-2025-04-14-1.738682

Dubai AI Week to welcome industry leaders, experts and officials from over a 100 countries

https://www.emirates247.com/technology/dubai-ai-week-to-welcome-industry-leaders-experts-and-officials-from-over-a-100-countries-2025-04-14-1.738653

Saudi Arabia rank 15 in AI research output

https://arab.news/bmfqr

Saudi tops the region in geospatial innovation!

https://lovin.co/riyadh/en/latest/saudi-jumps-to-9th-globally-and-tops-the-region-in-geospatial-innovation/

https://www.digitaldubai.ae/ar/knowledge-hub/publications/2025-

H.E. Younus Al Nasser, Chief Executive, Dubai Data and Statistics Establishment, Digital Dubai, emphasized that the State of AI in Dubai Report is based on global best practices and highlights over 100 real-world use cases of artificial intelligence. He also noted that the report presents practical steps to enhance AI’s positive impact on Dubai’s economic and social life, as well as overall quality of life.

Dubai State of AI Report 2025:
https://www.digitaldubai.ae/knowledge-hub/publications/dubai-state-of-ai-report-2025

At #DigitalDubai, our vision goes beyond digitalizing services, we’re building a connected digital ecosystem powered by AI; a system that thinks, learns, and interacts.
Starting April 21, stay tuned for our participation in Dubai AI Week 2025, an exceptional event aligned with the ambitions of the future.
Save the date.

For more information, visit:
https://week.dub.ai

#DubaiAIWeek2025
#DubaiFuture

Everything around you is digital and smart? That's normal.. because you're in Dubai

#DigitalDubai
#ActionFigure

IG:
https://www.instagram.com/reel/DIRlPAGTLv1/?igsh=MTEydXk4OXA3YnhmcA==

FB:

https://www.facebook.com/share/r/1Cpo6R8osa/?mibextid=wwXIfr

Tiktok:
https://vt.tiktok.com/ZSra9sQNs/

X:
https://x.com/digitaldubai/status/1910388169876386062?s=46&t=88GCW6UEFD4UlraCUj0yZA

LinkedIn:
https://www.linkedin.com/posts/digital-dubai_aexaeqaeyabraepaesaezaeqaetaeyaer-digitaldubai-activity-7316153323827412992-GTeN?utm_medium=ios_app&rcm=ACoAACq21lsBl5sUULnmvfiIw3b2qydSMBN2tb4&utm_source=social_share_send&utm_campaign=copy_link

Dubai will become the destination of choice for anyone hoping to play a leading role in the artificial intelligence sector, said Sheikh Hamdan. https://news.ae/3S4iwrs

Hamdan bin Mohammed directs Dubai AI Week to return in April 2026 with double the scale and global participation

https://www.emirates247.com/technology/hamdan-bin-mohammed-directs-dubai-ai-week-to-return-in-april-2026-with-double-the-scale-and-global-participation-2025-04-25-1.738948

Imperatives for Europe in the age of AI and automation, McKinsey (2017)

Artificial Intelligence for Europe, COM(2018) Coordinated Plan on Artificial Intelligence, COM(2018)

https://ec.europa.eu/jrc/en/publication/academic-offer-and-demand-advanced-profiles-eu

ec.europe.eu/digital-single-market/en/news/digital-innovation-hubs-helping-companies-across-economy-make-most- digital-opportunities.

www.Ai4eu.eu.

Europe.eu/investeu.

https://www.oecd.org/going-digital/ai/principles/

https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines

Artificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve

specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications)." High Level Expert Group, A definition of AI, : "Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions."

1-A summary of the national AI strategies of some countries can be found at: https://medium.com/politics-ai/an-overview-of-national-ai-strategies-2a70ec6edfd.

The following are examples of some of these strategies Denmark - Strategy for Denmark s Digital Growth- https://investindk.com/insights/the-danish-government-presents-digital-growth-strategy

EU Commission - Communication_Artificial_Intelligence forEurope https://ec.europa.eu/digital-singlemarket/en/news/communication-artificial-intelligence-europe France -

For a Meaningful Artificial Intelligence - Towards a French and European Strategy- https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf

Germany-Key points for a Federal Government Strategy on Artificial Intelligence https://www.bmwi.de/Redaktion/EN/Downloads/E/key-points-for-federal-government-strategy-onartificial-intelligence.pdf?__blob=publicationFile&v=4

NordicBaltic Region - Nordic-Baltic Region- Al in the Nordic-Baltic Region- https://www.regeringen.se/49a602/globalassets/regeringen/dokument/naringsdepartementet/20180 514_nmr_deklaration-slutlig-webb.pdf

UK Opportunities in the Al Industry - Sector Deal https://www.gov.uk/government/publications/artificial-intelligence-sector-deal

2. The term “Artificial Intelligence” was first used in 1956 and is attributed to John McCarthy, then a young assistant professor of mathematics at Dartmouth College, who organized a workshop named the “Dartmouth Summer Research Project on Artificial Intelligence” in the summer of 1956. McCarthy also co-invented the StarLisp programming language, which is popular in AI. An interesting perspective is provided by Jerry Kaplan’s informative 2016 book, “Artificial Intelligence: What everyone needs to know.”

3. Three highly popularized examples of AI defeating championship players in games of intelligence are IBM's Deep Blue defeating chess grandmaster Garry Kasparov in 1996, IBM's Watson defeating champions Brad Rutter and Ken Jennings in the quiz show Jeopardy! in 2011, and Google's AlphaGo defeating Go legend Lee Sedol in 2016

4. Qatar National Vision 2030 https://www.psa.gov.qa/en/qnv1/Documents/QNV2030_English_v2.pdf ;

5. University of Waterloo , Computer Science Lab

http://csclub.uwaterloo.ca/

Google and University of Waterloo AI challenge

https://web.archive.org/web/20101129201317/http://experimentgarden.blogspot.com/2010/02/google-university-of-waterloo-ai.html

6. A very good example of AI education for the broad population is Finland’s recent plan to teach 1% of the population the basics of AI: https://www.politico.eu/article/finland-one-percent-aiartificial-intelligence-courses-learning-training/

7. Qatar Data Privacy https://compliance.qcert.org/sites/default/files/library/202011/Law%20No.%20%2813%29%20of%202016%20%20on%20Protecting%20P

ersonal%20Data%2 0Privacy%20-%20English.pdf

8. Economist - The world’s most valuable resource is no longer oil, but data - https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-nolonger-oil-but-data

9. Carl Benedikt Frey and Michael A. Osborne, "The Future of Employment: How susceptible are jobs to computerisation?" Oxford Martin School Working Paper - https://www.oxfordmartin.ox.ac.uk/publications/view/1314 ;

10. “The AI Advantage – How to Put the Artificial Intelligence Revolution to Work” Thomas H. Davenport https://mitpress.mit.edu/books/ai-advantage

11. Planning and Statistics Authority - Labor Force Survey, Second Quarter (Q2) 2016 - https://www.psa.gov.qa/en/statistics1/pages/lateststats/20161012.aspx ;

12.Illustrated, bilingual manuscript about artificial neural networks; Topics so far: Perceptrons, Backpropagation, Radial Basis Functions, Recurrent Neural Networks, Self Organizing Maps, Hopfield Networks.

http://www.dkriesel.com/en/science/neural_networks

Werbos P (1975). Beyond Regression: New Tools for Prediction and Analysis in the Behavioral Sciences

https://books.google.com/books?id=z81XmgEACAAJ

13. Prediction Machines: The Simple Economics of Artificial Intelligence Hardcover, Avi Goldfarb https://www.amazon.com/Prediction-Machines-EconomicsArtificial-Intelligence/dp/1633695670/

14. "Artificial Intelligence: The Next Digital Frontier?" McKinsey Global Institute Discussion Paper, 2017 https://www.mckinsey.com/~/media/mckinsey/industries/advanced%20electronics/our%20insi ghts/how%20artificial%20intelligence%20can%20deliver%20real%20value%20to%20companies/ mgi-artificial-intelligence-discussion-paper.ashx

15. Examples of Qatar Digital Government services: - Qatar Digital Government – https://hukoomi.gov.qa/en/digital-project/qatar-digitalgovernment ; - Metrash for Ministry of Interior Services - https://portal.moi.gov.qa/wps/portal/MOIInternet/services/inquiries/metrash Qatar eGovernment Portal – Hukoomi – https://hukoomi.gov.qa/ ; -

Municipalities Services – http://www.mme.gov.qa/cui/view.dox?id=592&siteID=2 Oun application for municipalities services http://www.mme.gov.qa/cui/view.dox?id=743&siteID=2 ;

16. TASMU https://tasmu.gov.qa/

17. The social and ethical ramifications of AI are receiving significant attention from research and public policy

organizations. For example, the AI Now Institute at New York University (https://ainowinstitute.org/) has recently published a report outlining specific public policy recommendations to address ethical issues related to AI (https://ainowinstitute.org/AI_Now_2018_Report.pdf). The European Commission has drafted ethics guidelines for trustworthy AI (https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56433). These activities can inform the development of Qatar's strategy. However, it is important to note that many of the ethical issues related to AI have to be studied in the context of local cultural norms. For example, a recent Nature paper that studied people's perception of what constitutes ethical AI actions in a particular context revealed significant cultural and demographic variations in what people perceive as "the ethical thing to do" (https://www.nature.com/articles/s41586-018-0637-6) ;

18. EU General Data Protection Regulation (GDPR) - https://eugdpr.org/ ;

19. What is Edge AI ?

https://www.redhat.com/en/topics/edge-computing/what-is-edge-ai

20. Time to think beyond Cloud Computing.

https://www.wired.com/story/its-time-to-think-beyond-cloud-computing/

21. Edge Machine Learning for AI enabled devices.

https://www.satellitetoday.com/in-space-services/2023/05/12/size-of-the-prize-how-will-edge-computing-in-space-drive-value-creation/

Also , Which American Visionary Entrepreneur will revive , "The Sky Angel Networks and Broadcaster - a limited Liability Company ?

INDIA AI

Generated by Google Gemini Deep Research - INDIA AI

Multi-Modal Large Language Behavioural Generative AI Models in India: Development and Global Contributions

1. Introduction: Setting the Stage for India's AI Advancement
Artificial intelligence is rapidly evolving, with generative models and large language models at the forefront of this transformation. These advancements are not confined to specific regions but are increasingly recognized as pivotal for national development and technological independence across the globe. India, with its unique demographic and digital landscape, stands at a crucial juncture in harnessing the power of AI. This report aims to illuminate the current state of multi-modal large language behavioural generative AI models being developed from scratch within India.

Furthermore, it will explore the involvement of Indian AI startups and research organizations in the global open-source Artificial General Intelligence (AGI) development and evolution landscape, providing insights into India's contributions and potential in this cutting-edge field. The subsequent sections will delve into the specifics of MLLMs in the Indian context, the emergence of behavioural generative AI, the role of Indian startups and academic institutions, India's participation in global AGI efforts, and the challenges and opportunities that lie ahead.

2. Decoding Multi-Modal Large Language Models (MLLMs): The Indian Perspective

Multi-modal large language models represent a significant leap in artificial intelligence, extending the capabilities of traditional language models to process and generate content across diverse modalities. Unlike standard large language models that primarily focus on text, MLLMs can understand and produce information in various forms, including text, images, audio, and video. This integration of multiple data types allows MLLMs to achieve a more comprehensive understanding of the world and interact with it in more versatile ways, mirroring the multi-sensory nature of human cognition. The development of such sophisticated models is particularly significant for India, a nation characterized by immense linguistic and cultural diversity. Global AI models often fall short in adequately representing the nuances of Indian languages and cultural contexts. Therefore, the creation of indigenous MLLMs is essential to ensure that the benefits of AI are accessible to all segments of Indian society, fostering inclusivity and preserving the rich tapestry

of its cultural heritage. The BharatGen initiative, spearheaded by IIT Bombay under the National Mission on Interdisciplinary Cyber-Physical Systems, exemplifies India's commitment to advancing homegrown technologies in this domain. This government-funded project aims to develop a suite of foundational models in language, speech, and computer vision, explicitly prioritizing India's socio-cultural and linguistic diversity.

Developing AI models "from scratch" is a crucial aspect of achieving customization and technological sovereignty. This approach involves building the model architecture, training data, and tokenization processes specifically tailored to the intended use case and context. In the Indian scenario, building MLLMs from the ground up allows for a deeper integration of Indian languages and cultural understanding compared to merely fine-tuning existing models developed primarily for Western contexts. Fine-tuning might not fully capture the subtle nuances and specific requirements of Indian languages, potentially leading to inaccuracies or a lack of cultural relevance. Sarvam AI, a Bengaluru-based startup, is actively pursuing this strategy by developing large language models specifically optimized for India's linguistic diversity and unique use cases. This commitment to building models from scratch underscores the dedication to creating truly Indian AI solutions that can effectively address the nation's diverse needs.

3. The Rise of Behavioral Generative AI in India: Current Research and Applications

Behavioral generative AI refers to a category of artificial intelligence models that generate content influenced by or

designed with an understanding of human behavior, with the potential to even influence it. These models go beyond simply generating text or images; they aim to create outputs that are more personalized, engaging, and effective by considering the psychological and behavioral aspects of users. This capability holds immense potential for creating more intuitive and responsive AI interactions across various applications.
Current research trends in India indicate a growing interest in exploring the adoption and impact of AI, including its behavioral dimensions, across key sectors. Academic institutions are actively involved in studying how individuals interact with AI technologies and the factors that influence their acceptance. For instance, studies have explored the behavioral intentions of students in Tier II cities towards adopting AI-based learning platforms, highlighting the significant role of social influence and facilitating conditions in technology adoption. Furthermore, research is also focusing on the application of AI in sensitive areas like mental health interventions within the Indian context, examining user perceptions, trust levels, and potential benefits such as increased accessibility and reduced stigma associated with seeking help.
Behavioral generative AI has the potential to revolutionize several key sectors in India. In the financial domain, generative AI is being explored for its ability to create hyper-

personalized customer experiences and implement behavioral nudges to improve financial health outcomes. These models can analyze spending patterns and other behavioral cues to offer tailored advice and interventions. The banking sector in India, with its diverse economic and regulatory challenges, can leverage this technology to push

the boundaries of financial inclusion and enhance data-driven credit assessment. In education, behavioral generative AI can facilitate the creation of adaptive learning platforms that tailor content and delivery methods to individual student needs and learning styles, potentially improving engagement and outcomes. The healthcare sector also stands to benefit significantly, with potential applications in providing personalized health recommendations, supporting mental well-being through empathetic AI agents, and even assisting in early diagnosis through behavioral and linguistic analysis. The ability of these models to understand and respond to human emotions and behaviors opens up new avenues for creating AI solutions that are more human-centric and impactful.

4. Indian AI Startups Spearheading LLM Innovation: From Foundation Models to Applications

A dynamic ecosystem of Indian AI startups is emerging as key drivers of innovation in large language models, with a particular focus on addressing the unique linguistic needs of the country. Several companies are making significant strides in developing LLMs that support various Indian languages, moving beyond the dominance of English-centric models. Sarvam AI, founded by experts with deep roots in India's digital infrastructure and AI research, is building LLMs

from the ground up, specifically optimized for Indian languages and use cases. Their open-source model, Sarvam 2B, trained on a massive dataset of 4 trillion tokens, supports 10 Indian languages, focusing on tasks like translation and summarization. Krutrim, backed by Ola founder Bhavish Aggarwal, is another prominent player, having developed

India's first homegrown large language model trained on extensive datasets of Indian languages and contextual data, capable of handling text, speech, and vision-based tasks. Tech Mahindra's Project Indus represents an effort by a major Indian IT giant to create an open-source AI model designed to enhance enterprise solutions with a focus on Indian languages. Gyan AI's Paramanu series offers lightweight AI models optimized for several Indian languages, requiring fewer computational resources while delivering high performance. These startups are demonstrating that significant advancements in AI are achievable in India, even challenging the notion that competing with global AI leaders requires insurmountable resources.

Open-source development is a central strategy employed by many of these Indian AI startups to democratize access to AI and foster innovation within the country. BharatGen, the government-funded initiative led by IIT Bombay, emphasizes the development of an open-source platform to create an ecosystem for generative AI research in India. Tech Mahindra's Project Indus is also available as an open-source model on platforms like Hugging Face. Soket AI Labs achieved a significant milestone by launching Pragna-1B, India's first open-source multilingual foundation model, supporting vernacular languages like Hindi, Bengali, and Gujarati. This commitment to open-source principles allows researchers, developers, and other startups to build upon existing work, accelerating the creation of AI solutions tailored for the Indian context. The availability of these models and related resources as public goods helps to lower the barrier to entry for innovation and encourages collaboration across the AI community in India.

Indian AI startups are also making notable progress in building models with diverse capabilities, including multilingual support and the ability to handle different modalities. Krutrim's suite of models, including Krutrim-1 and Krutrim-2 (large language models), Chitrarth-1 (vision-language model), Vyakyarth-1 (Indic embedding model), and Dhwani-1 (speech large language model), showcases the ability to handle text, speech, and vision in multiple Indian languages. Sarvam AI's models, such as Sarvam 2B and Shuka v1 (an open-source audio language model), focus on providing robust capabilities for translation, summarization, and speech understanding in various Indian languages. These developments indicate a clear trend towards building truly multilingual and multimodal AI systems that can effectively serve India's diverse population and address a wide range of applications, from customer service automation to content creation and beyond.

5. Academic and Research Institutions Driving Generative AI in India: Contributions and Collaborations

Premier Indian academic and research institutions play a pivotal role in advancing the frontiers of generative AI research and development. These institutions provide the foundational knowledge, talent, and infrastructure necessary to drive innovation in this rapidly evolving field. IIT Bombay is at the helm of the ambitious BharatGen initiative, a government-funded project aimed at creating multimodal LLMs for public service delivery and citizen engagement. IIT Madras is home to AI4Bharat, a leading research lab dedicated to advancing AI technology for Indian languages through open-source contributions, developing a wide array

of datasets, tools, and state-of-the-art models. IIIT Hyderabad has established a dedicated Kohli Centre on Intelligent Systems, actively involved in creating and publishing local datasets and contributing to AI policy development. These institutions, along with others like IIT Kanpur, IIT Kharagpur, and the Indian Institute of Science (IISc), are fostering a vibrant research ecosystem in generative AI.

These academic institutions are also engaged in specific research projects, leading to the creation of valuable datasets and innovative models. Researchers at IIT Patna have developed MedSumm, a novel multimodal framework and dataset for summarizing medical queries in Hindi-English code-mixed language, integrating visual information for a more holistic understanding of patient conditions. AI4Bharat has developed IndicTrans2, a high-quality machine translation model for all 22 scheduled Indian languages, along with extensive training datasets. Numerous academic papers published by Indian researchers showcase advancements in multimodal LLMs for Indic languages, including models like Chitranuvad, which effectively integrates multilingual LLMs with vision modules for tasks like multimodal translation. These contributions are crucial for addressing the specific challenges and opportunities presented by India's linguistic and cultural diversity, including domain-specific applications in areas such as healthcare and agriculture.

Collaboration between academia, industry, and government is proving to be a vital catalyst for driving AI innovation in India. IndiaAI, a collaborative initiative under the Ministry of Electronics and Information Technology (MeitY), has partnered with Meta to establish centers for generative AI,

named Srijan, at IIT Jodhpur, aiming to empower students and young developers in this field. Sarvam AI has announced a significant partnership with NVIDIA, leveraging their advanced computing infrastructure for developing and training their multilingual LLMs. The AI Alliance, a global community dedicated to advancing safe and responsible AI, includes several prominent Indian academic institutions like AI4Bharat (IIT Madras) and IIT Jodhpur, alongside startups like Sarvam AI, fostering collaboration and knowledge sharing. These collaborations are essential for translating cutting-edge research into practical applications, bridging the gap between theoretical advancements and real-world impact, and building a robust and interconnected AI ecosystem in India.

6. India's Footprint in Global Open-Source AGI Development: Participation and Impact

Artificial General Intelligence (AGI) represents the aspiration to create AI systems with human-level cognitive abilities, capable of performing a wide range of intellectual tasks with proficiency. While the field is still in its nascent stages, there is a growing global movement towards open-source AGI development, aiming to democratize access and foster collaborative innovation. Several Indian AI startups and research organizations are beginning to make their mark in this ambitious domain. Soket AI Labs, based in Bengaluru and Gurugram, has explicitly stated its aim to build solutions towards achieving ethical AGI, starting with smaller language models and progressively developing more advanced AI systems. Sandeep Nailwal, co-founder of Polygon, has launched Sentient, a blockchain-based AI startup focused on

developing open-source decentralized AI and eventually AGI, leveraging blockchain incentives to reward community contributions. Olbrain Labs, with entities registered in both Delaware and Gurgaon, India, is another pioneering research and product company actively building next-generation AI architectures, agents, and platforms with the goal of achieving AGI, specifically tailored for India's diverse business landscape.

While the direct involvement of Indian entities in established global open-source AGI labs might be limited at this stage, their contributions to the broader open-source AI community are significant and growing. India has emerged as the second-largest contributor to AI-related projects on GitHub, underscoring the presence of a large and active developer base engaged in open innovation. Open-source projects originating from India, such as ERPNext (an enterprise resource planning software) and AI4Bharat's language models and datasets, are gaining global traction and contributing to the collective knowledge and resources within the AI community. This strong foundation in open-source AI development positions India well to potentially play a more prominent role in open-source AGI efforts in the future. Collaborations and partnerships between Indian AI entities and international open-source AGI development initiatives are also beginning to emerge. SingularityNET, a decentralized

AI platform with a vision towards AGI, has partnered with Bitgrit, a global network of AI/ML engineers, to accelerate the development and adoption of AGI, with a specific focus on advancing SingularityNET's open-source AGI framework, OpenCog Hyperon. This collaboration connects a vast pool of global AI talent to an AGI project with Indian participation.

Furthermore, Indian organizations like AI4Bharat and Sarvam AI are members of the AI Alliance, a global initiative that champions an open, safe, and responsible approach to AI development, which includes exploring pathways towards more advanced forms of artificial intelligence. These collaborations facilitate the exchange of knowledge, resources, and expertise, fostering a more open and inclusive global AI ecosystem.

7. Challenges and Opportunities for India in Advanced AI Development

India's journey towards becoming a global leader in advanced AI development, particularly in building models from scratch, is fraught with several challenges. Access to substantial compute resources, especially high-end GPUs necessary for training large and complex models, remains a significant hurdle. Restrictions on the export of advanced GPUs to India can further exacerbate this issue. Another critical challenge is the availability of large volumes of high-quality, India-specific data required to train models that truly understand the nuances of Indian languages, culture, and context. While India has a vast digital footprint, much of this data is locked within platforms owned by global tech firms, limiting access for Indian startups and researchers. Furthermore, there is a need to nurture and retain top-tier AI

research talent within the country. Many promising AI researchers trained in India often end up working in the United States or Europe after completing their higher education, contributing to a talent outflow.

Despite these challenges, India possesses several unique strengths and opportunities in the realm of advanced AI

development. The country boasts a vast and rapidly growing pool of software engineers and developers, representing a significant talent advantage. The Indian government is actively promoting AI through strategic initiatives like the IndiaAI mission, which aims to build a comprehensive ecosystem for AI innovation, including the development of AI infrastructure and support for domestic AI models and startups. India's digital infrastructure is also undergoing rapid development, with increasing investments in data centers and cloud computing capabilities, which are essential for supporting AI workloads. This combination of a large talent pool, government support, and developing infrastructure provides a strong foundation for growth in advanced AI.
India has a unique opportunity to focus on its inherent strengths, particularly in the development of multilingual AI and AI for social good. The BharatGen initiative's explicit focus on India's linguistic diversity and socio-cultural context highlights this strategic direction. Unlike many nations primarily pursuing AI for commercial or military gains, India can chart a distinct path by leveraging AI to address pressing socio-economic challenges and improve public welfare. By focusing on building AI models that understand and operate in the multitude of Indian languages and by applying AI to solve problems in sectors like healthcare, agriculture, and

education, India can establish itself as a leader in creating AI solutions that are both innovative and impactful for its diverse population.

8. Conclusion: India's Journey Towards AI Sovereignty and Global Contribution

India is making significant strides in the development of multi-

modal large language behavioural generative AI models from scratch, driven by a combination of ambitious government initiatives, innovative startups, and dedicated academic institutions. The focus on addressing the country's unique linguistic and cultural diversity is evident in projects like BharatGen and the efforts of startups like Sarvam AI and Krutrim. While India's direct participation in global open-source AGI development labs is still in its early stages, the nation's strong and growing contributions to the broader open-source AI community, particularly on platforms like GitHub, indicate a solid foundation for future involvement. Despite facing challenges such as access to compute resources and high-quality data, India's vast talent pool, increasing digital infrastructure, and proactive government support provide a strong impetus for growth in advanced AI. By strategically focusing on its unique strengths in multilingual AI and AI for social good, India has the potential to emerge as a significant player in the global AI landscape, contributing not only to its own technological sovereignty but also to the advancement of AI for the benefit of all. The journey is ongoing, but the momentum and direction suggest a promising future for India in the realm of advanced artificial intelligence.

Table 1: Key Indian AI Startups Developing Large Language Models

Startup Name	Focus Area	Notable Models	Open-Source Involvement	Key Collaborations
Sarvam AI	Multilingual LLMs, Voice-First AI	Sarvam 2B, Shuka v1	Sarvam 2B, Shuka v1	NVIDIA, Yotta Data Services

Krutrim	Multilingual & Multimodal LLMs, AI Chips	Krutrim-1, Krutrim-2, Chitrarth-1, Vyakyarth-1, Dhwani-1	Krutrim-1, Krutrim-2, Chitrarth-1, Vyakyarth-1, Dhwani-1	Microsoft, NVIDIA
Tech Mahindra	Multilingual LLMs for Enterprise	Project Indus	Project Indus	
Gyan AI	Lightweight Multilingual LLMs	Paramanu series		
Yellow.ai	Proprietary LLM for Enterprise Automation	YellowG		
Uniphore	Conversational AI for Customer Service	Conversational AI models		
Hanooman AI	Multimodal LLMs	Hanooman		IIT Bombay, Reliance Jio
CoRover.ai	Multilingual Virtual Assistants	BharatGPT		
AI4Bharat	Machine Translation for Indic Languages	IndicTrans2, IndicBERT, IndicBART, Airavata, IndicXlit, IndicWav2Vec, AI4BTTS	Wide range of open-source models and datasets	Meta, Bhashini (MeitY)
Soket AI Labs	Multilingual Foundation Models, Ethical AGI	Pragna-1B	Pragna-1B	Google Cloud

Table 2: Major Indian Academic and Research Institutions Involved in Generative AI Research

Institution Name	Key Research Areas in Generative AI	Notable Projects/Datasets/Models	Collaboration Highlights
IIT Bombay	Multimodal LLMs, Generative AI for Public Service	BharatGen initiative	IIIT Hyderabad, IIT Mandi, IIT Kanpur, IIT Hyderabad, IIM Indore, IIT Madras
IIT Madras	Multilingual LLMs, Machine Translation, Speech

Recognition, Text-to-Speech | IndicTrans2, IndicBERT, IndicBART, Airavata, IndicXlit, IndicWav2Vec, AI4BTTS, extensive datasets | AI Alliance, Meta, Bhashini (MeitY) |
IIIT Hyderabad	Multilingual LLMs, AI Policy	Indian languages datasets, Indian traffic dataset	IIT Bombay (BharatGen)
IIT Patna	Multimodal Medical Question Summarization	MedSumm framework and dataset	Indira Gandhi Institute of Medical Sciences, Amazon Generative AI, Stanford University
IIT Jodhpur	Generative AI, Foundation Models	Research in ethical and inclusive AI	AI Alliance, Meta (Srijan Center)
Indian Institute of Science (IISc)	Deep Learning, AI in Healthcare, Robotics	Postgraduate program in AI, research in various AI domains	Wipro (AI-driven health behavior innovations), Kotak IISc AI–ML Centre

Table 3: IndiaAI Mission Pillars and Focus Areas

Pillar Name	Key Objectives	Relevance to Generative AI and AGI
IndiaAI Compute Capacity	Build scalable AI ecosystem with 10,000+ GPUs via public-private partnerships	Provides the necessary computational power for training large generative models and potentially AGI systems.
IndiaAI Innovation Centre	Develop and deploy indigenous Large Multimodal Models and domain-specific foundational models	Directly supports the creation of MLLMs and foundational models, a key focus of this report.
IndiaAI Datasets Platform	Streamline access to high-quality non-personal datasets for AI innovation	Addresses the critical challenge of data availability for training effective generative models.

IndiaAI Application Development Initiative	Develop, scale, and promote impactful AI solutions for large-scale socio-economic transformation	Provides a pathway for deploying generative AI models to address real-world problems.
IndiaAI FutureSkills	Expand AI education at all academic levels and establish Data and AI Labs in Tier 2 and 3 cities	Ensures a pipeline of talent equipped to develop and utilize advanced AI, including generative models and AGI.
IndiaAI Startup Financing	Accelerate deep-tech AI startups by streamlining access to funding for innovative AI projects	Supports the growth of startups working on generative AI and potentially AGI.
Safe & Trusted AI	Ensure responsible AI via projects, tools, checklists, and governance frameworks	Addresses the ethical considerations crucial for the development and deployment of advanced AI.

Moneycontrol: Watch | Ashwini Vaishnaw showcases India’s first fully designed AI server

https://www.moneycontrol.com/news/india/watch-ashwini-vaishnaw-showcases-india-s-first-fully-designed-ai-server-adipoli-12998156.html

Analytics India Magazine: Microsoft Unveils 1-Bit Compact LLM that Runs on CPUs

https://analyticsindiamag.com/ai-news-updates/microsoft-unveils-1-bit-compact-llm-that-runs-on-cpus/

I'm doing well, thank you for asking! It's fascinating to discuss the advancements in AI happening in India. Let's delve into the exciting world of multimodal large language behavioral generative AI models being developed in India and explore the involvement of Indian entities in global open-source AGI development.

Multimodal Large Language Behavioral Generative AI Models in India

India is increasingly becoming a hub for the development of sophisticated AI models, including those that are multimodal, large language models with a focus on behavior and generative capabilities. These models aim to understand and generate content across various modalities like text, speech, and potentially vision, while also being attuned to behavioral nuances, particularly within the Indian context.

Here's a glimpse into some key initiatives and trends:

* BharatGen: This is a significant government-backed initiative, hailed as the world's first government-funded multimodal large language model project. Spearheaded by IIT Bombay under the National Mission on Interdisciplinary Cyber-Physical Systems of the Department of Science and Technology , BharatGen aims to:
  * Develop foundational AI models in language, speech, and computer vision.
  * Revolutionize public service delivery and enhance citizen engagement.
  * Prioritize India's socio-cultural and linguistic diversity by training on multilingual datasets to capture the nuances of Indian languages.
  * Foster an open-source platform to encourage AI research and innovation within the country.

  * Align with the "Atmanirbhar Bharat" (self-reliant India) vision by reducing reliance on foreign technologies.
* IndiaAI Mission: This broader government initiative is also driving the development of indigenous AI models. As part of this, a call for proposals was launched in January 2025, inviting startups, researchers, and entrepreneurs to collaborate on building state-of-the-art foundational AI models trained on Indian datasets. A significant number of these proposals focus on Large Language Models (LLMs) and Large Multimodal Models (LMMs).
* Startup Innovation: Several Indian AI startups are actively building their own large language models, some with multimodal aspirations:
  * Krutrim AI: Founded by Bhavish Aggarwal of Ola Cabs, Krutrim has developed a generative AI assistant capable of conversing in over 10 Indian languages. While the initial focus is on language, they have indicated plans to build multimodal models across text, voice, and vision. Krutrim Pro, a large multimodal model, is reportedly under R&D.
  * Sarvam AI: This startup has launched open-source foundational models supporting multiple Indian languages, such as Sarvam 2B. Their platform is designed to be voice-enabled and multilingual, with a focus on making AI accessible across India's linguistic diversity. They have also released models like OpenHathi, designed to empower diverse applications in the Indian market.

  * Gyan AI: They have built lightweight AI models (Paramanu family) optimized for Indian languages, demonstrating strong performance with fewer computational resources.
  * Tech Mahindra's Project Indus: This is an open-source model focused on Indian languages, aiming to improve

enterprise AI solutions.
* Academia and Research: Premier academic institutions like IIT Bombay, IIIT Hyderabad, IIT Mandi, IIT Kanpur, IIT Madras, and IIM Indore are key collaborators in the BharatGen initiative, contributing their research expertise to develop these advanced models.
These efforts signify a strong push towards creating AI that is not only technologically advanced but also culturally and linguistically relevant to India's diverse population.
Indian Participation in Global Open Source AGI Development
Regarding Indian AI startups and research organizations participating in global open-source Artificial General Intelligence (AGI) development and evolution labs, the landscape is still evolving. While there isn't extensive information readily available about large-scale, direct Indian participation in the most prominent global open-source AGI labs (if such centralized labs exist in a widely recognized form), there are indicators of involvement and contributions in related areas:
* Open Source Model Contributions: Indian startups and research entities are increasingly releasing their AI models and datasets in the open-source domain. For example, Sarvam AI has open-sourced models like Sarvam 2B and the OpenHathi series. Tech Mahindra's Project Indus is also available on platforms like Hugging Face. This sharing of resources contributes to the global pool of AI knowledge and development.
* Collaborations and Partnerships: Indian researchers and startups may be engaging in collaborations with international researchers and institutions that are involved in AGI-related research. The BharatGen initiative itself mentions

partnerships with research groups across the country, which could potentially extend to international collaborations in the future.
* Talent Pool: Many AI researchers and engineers globally are of Indian origin, and their contributions to various international labs and open-source projects indirectly represent Indian intellect and expertise in the field, even if not under the banner of an Indian organization.
* Focus on Applied AI: Currently, the emphasis in the Indian AI ecosystem appears to be strongly on building practical AI solutions tailored to Indian needs, including language models and multimodal systems. While this might not always translate directly into participation in fundamental AGI research labs, the foundational work being done on these models could contribute to the broader progress towards AGI.
* Emerging Initiatives: As the AI landscape matures in India, we might see more dedicated efforts and collaborations focused specifically on open-source AGI research. Initiatives like the IndiaAI mission could potentially foster such engagements in the future.
It's important to note that the definition and structure of "global open source Artificial General Intelligence development and evolution labs" might be somewhat fluid. AGI research is a complex and long-term endeavor, often involving distributed collaborations rather than centralized labs. Indian contributions might be more visible through

open-source releases, research publications, and participation in international AI conferences and communities.
In conclusion, India is making significant strides in developing its own multimodal large language behavioral

generative AI models, driven by government initiatives, innovative startups, and academic research. While direct, large-scale participation of Indian entities in explicitly named "global open source AGI development and evolution labs" might not be widely documented yet, the increasing open-sourcing of Indian AI models and the growing talent pool suggest a valuable, albeit potentially distributed, contribution to the global AI advancement, which includes the long-term pursuit of AGI.

SARVAM AI - India's homegrown AI model

https://indianexpress.com/article/business/centre-selects-start-up-sarvam-to-build-country-first-homegrown-ai-model-9967243/

Indian IT outsourcing companies, which employ millions, are tapping AI to boost efficiency and reduce the need for more workers to grow their business.

https://bloom.bg/4ixeRgH

The Indian Express: 60% Indians unfamiliar with AI: Google-Kantar study as Gemini hits 350M users globally

https://indianexpress.com/article/technology/artificial-intelligence/google-kantar-study-ai-adoption-india-gemini-day-2025-9965664/

GigEagle and the DoD’s Agile Talent Ecosystem Receives Scaling Investment from CDAO > Dobbins Air Reserve Base > Article Display
https://www.dobbins.afrc.af.mil/News/Article-Display/Article/4017018/gigeagle-and-the-dods-agile-talent-ecosystem-receives-scaling-investment-from-c/

Full article: The Impact of Military Expenditures on Economic Growth: A New Instrumental Variables Approach
https://www.tandfonline.com/doi/full/10.1080/10242694.2023.2259651#d1e943

Full article: On the role of military spending: an economic thought perspective
https://www.tandfonline.com/doi/full/10.1080/23311886.2024.2350837#d1e225

World military expenditure reaches new record high as European spending surges | SIPRI
https://www.sipri.org/media/press-release/2023/world-military-expenditure-reaches-new-record-high-european-spending-surges

SIPRI Military Expenditure Database | SIPRI

https://www.sipri.org/databases/milex

Glossary | DataBank
https://databank.worldbank.org/metadataglossary/world-development-indicators/series/MS.MIL.XPND.GD.ZS

How much does the US spend on the military? | USAFacts
https://usafacts.org/articles/how-much-does-the-us-spend-on-the-military/

Chart: The Most Important Network Infrastructure Providers Worldwide | Statista
https://www.statista.com/chart/31093/global-market-share-of-network-infrastructure-providers/

Chart: U.S. and China Dominate the Data Center Market | Statista
https://www.statista.com/chart/30940/data-center-revenue-by-country/

World's Top 10 Internet Companies
https://www.investopedia.com/articles/personal-finance/030415/worlds-top-10-internet-companies.asp

Network Infrastructure Market: Industry Analysis & Forecast 2030
https://www.maximizemarketresearch.com/market-report/global-network-infrastructure-market/23874/

Top 20 Information Technology Countries in the World

https://finance.yahoo.com/news/top-20-information-

technology-countries-130614172.html

Global Digital Infrastructure Market Size, Trends,Share 2032
https://www.custommarketinsights.com/report/digital-infrastructure-market/

The 25 Largest Internet Companies In The World - WorldAtlas
https://www.worldatlas.com/articles/the-25-largest-internet-companies-in-the-world.html

Global Wireless Infrastructure Market Size To Worth USD
https://www.globenewswire.com/news-release/2024/03/22/2850859/0/en/Global-Wireless-Infrastructure-Market-Size-To-Worth-USD-401-9-Billion-By-2033-CAGR-of-8-56.html

Enterprise Network Infrastructure Market Size, Report By 2034
https://www.precedenceresearch.com/enterprise-network-infrastructure-market

Top 25 Biggest Internet Companies in the US - Insider Monkey
https://www.insidermonkey.com/blog/top-25-biggest-internet-companies-in-the-us-1286779/

Global Telecom Network Infrastructure Market Size, Share.
https://www.sphericalinsights.com/reports/telecom-network-infrastructure-market

AI Agents in Diplomacy – Promoting Stability or Chaos? | The Belfer Center for Science and International Affairs
https://www.belfercenter.org/publication/ai-agents-diplomacy-promoting-stability-or-chaos

Enhancing the Intelligence Cycle: How to Leverage Feedback to Provide More Valuable Intelligence | The Belfer Center for Science and International Affairs
https://www.belfercenter.org/research-analysis/enhancing-intelligence-cycle-how-leverage-feedback-provide-more-valuable

Trump promises $1 trillion in defense spending for next year
https://www.militarytimes.com/news/pentagon-congress/2025/04/08/trump-promises-1-trillion-in-defense-spending-for-next-year/

Full article: AI and the decision to go to war: future risks and opportunities
https://www.tandfonline.com/doi/full/10.1080/10357718.2024.2349598#abstract

Center for European Policy Analysis

https://cepa.org/

CyberUSA
https://www.cyberusa.us/

DARPA exploring ways to assess ethics for autonomous

weapons | DARPA
https://www.darpa.mil/news/2024/asimov-approaches

Open-Source Intelligence and the Challenges of Overclassification | Lawfare
https://www.lawfaremedia.org/article/open-source-intelligence-and-the-challenges-of-overclassification

Cybersecurity Predictions for 2025: Challenges and Opportunities - National Cybersecurity Alliance
https://www.staysafeonline.org/articles/cybersecurity-predictions-for-2025-challenges-and-opportunities

How the DOD is enabling its Zero Trust mission | Security Info Watch
https://www.securityinfowatch.com/cybersecurity/information-security/article/55260306/how-the-dod-is-enabling-its-zero-trust-mission

Countries with the largest petroleum reserves in the world

https://geologyscience.com/geology-branches/petroleum-geology/countries-with-the-largest-petroleum-reserves-in-the-world/

The World's Largest Oil Reserves by Country In 2024 - WorldAtlas
https://www.worldatlas.com/industries/the-world-s-largest-oil-reserves-by-country.html?utm_source=chatgpt.com

Natural Gas Reserves By Country December 2022
https://www.theworldranking.com/statistics/229/natural-gas-reserves/?utm_source=chatgpt.com

Which Countries Have the World's Largest Proven Oil Reserves?
https://www.visualcapitalist.com/ranking-the-countries-with-the-largest-proven-global-oil-reserves-in-the-world/

Arms Transfers: U.S. and Russia’s Biggest Trading Partners
https://www.visualcapitalist.com/cp/arms-transfers-u-s-and-russias-biggest-trading-partners/

US Army taps CACI-owned company for jamming kit that troops can carry
https://www.c4isrnet.com/industry/2023/09/18/us-army-taps-caci-owned-company-for-jamming-kit-that-troops-can-carry/

Electronic warfare training is headed to an Army school near you
https://www.armytimes.com/news/your-army/2023/10/06/electronic-warfare-training-is-headed-to-an-army-school-near-you/

British soldiers take down drone swarm in groundbreaking use of radio wave weapon - GOV.UK

https://www.gov.uk/government/news/british-soldiers-take-down-drone-swarm-in-groundbreaking-use-of-radio-wave-weapon

Learn the Secret Histories of These Fascinating CIA Artifacts, From Pigeon Cameras to Cufflink Compasses | Smithsonian
https://www.smithsonianmag.com/smart-news/learn-the-secret-histories-of-these-fascinating-cia-artifacts-from-pigeon-cameras-to-cufflink-compasses-180986155/

Axios' “Zero Day” and the Case for Enhanced U.S. Cybersecurity
https://axioszerodayandthecaseforenhan.splashthat.com/?lid=hlzjmewbur8f

Cyber Command 2.0 Eyes Creation of a Cyber Innovation Warfare Center | AFCEA International
https://www.afcea.org/signal-media/cyber-edge/cyber-command-20-eyes-creation-cyber-innovation-warfare-center

SpaceX, ULA, Blue Origin win $13.7 billion in U.S. military launch contracts through 2029 - SpaceNews
https://spacenews.com/spacex-ula-blue-origin-win-13-5-billion-in-u-s-military-launch-contracts-through-2029/

DoD interested in smartphone-to-satellite communications services - SpaceNews
https://spacenews.com/dod-interested-in-smartphone-to-

satellite-communications-services/

A $1 trillion defense budget? Trump, Hegseth say it's happening - Breaking Defense
https://breakingdefense.com/2025/04/a-1-trillion-defense-budget-trump-hegseth-say-its-happening/

Ranked: The 15 Largest Defense Budgets in the World
https://www.visualcapitalist.com/largest-defense-budgets-in-the-world/#:~:text=Visualizing%20the%20Largest%20Defense%20Budgets%20in%20the%20World&text=In%202024%2C%20the%20U.S.%20spent,2%25%20of%20GDP%20on%20defense.

Palantir wins contract to expand access to Project Maven AI tools
https://www.c4isrnet.com/artificial-intelligence/2024/05/30/palantir-wins-contract-to-expand-access-to-project-maven-ai-tools/

United States' Project Maven And The Rise Of AI-Assisted Warfare — Global Defense Insight
https://defensetalks.com/united-states-project-maven-and-the-rise-of-ai-assisted-warfare/

British soldiers take down drone swarm in groundbreaking use of radio wave weapon - GOV.UK
https://www.gov.uk/government/news/british-soldiers-take-

down-drone-swarm-in-groundbreaking-use-of-radio-wave-weapon

British soldiers take down drone swarm in groundbreaking use of radio wave weapon - GOV.UK
https://www.gov.uk/government/news/british-soldiers-take-down-drone-swarm-in-groundbreaking-use-of-radio-wave-weapon

Cognitive warfare: the new battlefield exploiting our brains
https://www.polytechnique-insights.com/en/columns/geopolitics/cognitive-warfare-the-new-battlefield-exploiting-our-brains/

Is this unit the future of Army combat formations?
https://www.armytimes.com/news/your-army/2024/07/30/is-this-unit-the-future-of-army-combat-formations/

Army taps ‘Ghost Fleet’ authors to write novel on multi-domain warfare
https://www.militarytimes.com/news/your-military/2024/11/19/army-taps-ghost-fleet-authors-to-write-novel-on-multi-domain-warfare/

Interpreting India’s Cyber Statecraft | Carnegie Endowment for International Peace
https://carnegieendowment.org/research/2025/03/interpreting-indias-cyber-statecraft?lang=en&s=08

The United States has technology that allows you to control time and space — Kratsios — EADaily, April 16th, 2025 — Politics, USA

https://eadaily-com.cdn.ampproject.org/v/s/eadaily.com/en/ampnews/2025/04/16/the-united-states-has-technology-that-allows-you-to-control-time-and-space-kratsios

White House Says It Has Tech That Can 'Manipulate Time and Space' - Newsweek
https://www.newsweek.com/white-house-says-tech-can-manipulate-time-space-2060986

America can 'manipulate time and space', says Trump science chief
https://interestingengineering.com/science/trump-advisor-says-american-can-bend-time

Trump's Tech Chief Claims US Can 'Manipulate' Time And Space - Benzinga
https://www.benzinga.com/tech/25/04/44881790/trumps-tech-chief-claims-us-can-manipulate-time-and-space

US accelerates development of new B61-13 nuclear gravity bomb to expand strategic attack options
https://armyrecognition.com/news/army-news/2025/us-accelerates-development-of-new-b61-13-nuclear-gravity-bomb-to-expand-strategic-attack-options

Project Convergence Capstone 5 experiments at NTC
https://www-army-mil.cdn.ampproject.org/c/s/

www.army.mil/article-amp/284397/project_convergence_capstone_5_experiments_at_ntc

Time for Space Force to 'clearly say' it needs 'weapons in space': SPACECOM head - Breaking Defense
https://breakingdefense.com/2025/04/time-for-space-force-to-clearly-say-it-needs-weapons-in-space-spacecom-head/

Hegseth issues edict on DOD software acquisition | DefenseScoop
https://defensescoop.com/2025/03/07/hegseth-memo-dod-software-acquisition-pathway-cso-ota/?utm_content=326786855&utm_medium=social&utm_source=linkedin&hss_channel=lcp-80356765

It begins: Pentagon to give AI agents a role in decision making, ops planning • The Register
https://www.theregister.com/AMP/2025/03/05/dod_taps_scale_to_bring/

Pentagon signs AI deal to aid military decision-making
https://thehill.com/policy/technology/5178088-pentagon-signs-ai-deal-to-aid-military-decision-making/amp/

Pentagon Selects Scale AI to Support AI-Driven Military Planning, Decision-Making
https://thedefensepost.com/2025/03/06/pentagon-ai-military-planning/amp/

Pentagon to build AI for war planning in Europe and Asia -

Defense One
https://www.defenseone.com/technology/2025/03/pentagon-build-ai-war-planning-europe-and-asia/403506/

AI for war plans: Pentagon innovation shop taps Scale AI to build 'Thunderforge' prototype - Breaking Defense

http://breakingdefense.com/2025/03/ai-for-war-plans-pentagon-innovation-shop-taps-scale-ai-to-build-thunderforge-prototype/

Pentagon to build AI for war planning in Europe and Asia - Defense One
https://www.defenseone.com/technology/2025/03/pentagon-build-ai-war-planning-europe-and-asia/403506/

Pentagon contract ‘Thunderforge’ will make AI tools for military planning - The Washington Post
https://www.washingtonpost.com/technology/2025/03/05/pentagon-ai-military-scale/

pentagon AI role in decision planning and operations - Google Search
https://www.google.com/search?ie=UTF-8&client=ms-android-samsung-rvo1&source=android-browser&q=pentagon+AI+role+in+decision+planning+and+operations&sei=3EHKZ9aDGL_dseMPwevukQ4

Pentagon to give AI agents a role in planning, operations • The Register
https://www.theregister.com/2025/03/05/

dod_taps_scale_to_bring/

Promoting Resilience, Manufacturing for the Future of Defense Technology
https://www.diu.mil/latest/senior-leaders-promote-resilience-manufacturing-as-keys-to-the-future-of

Why AI Can't Replace Cybersecurity Analysts
https://www.linkedin.com/pulse/why-ai-cant-replace-cybersecurity-analysts-lesley-carhart-18l5c

Navigating the AI Frontier: Analysis of the 2025 Paris AI Action Summit – Center For Land Warfare Studies (CLAWS)
https://www.claws.in/navigating-the-ai-frontier-analysis-of-the-2025-paris-ai-action-summit/

Evolving Global Cyber Defence: The Impact and Implications of the UN Cybercrime Convention – Center For Land Warfare Studies (CLAWS)
https://www.claws.in/advancing-global-cyber-defense-the-impact-and-implications-of-the-un-cybercrime-convention/

Momentous Changes: Defence Reforms, Military Transformation, and India’s New Strategic Posture
https://www.orfonline.org/research/momentous-changes-defence-reforms-military-transformation-and-india-s-new-strategic-posture

JUST IN: Trump Revives Reagan’s ‘Star Wars' Missile Defense Aspirations

https://www.nationaldefensemagazine.org/articles/2025/1/28/just-in-trump-revives-reagans-star-wars-missile-defense-aspirations

Dilemmas in the policy debate on autonomous weapon systems | SIPRI
https://www.sipri.org/commentary/topical-backgrounder/2025/dilemmas-policy-debate-autonomous-weapon-systems

Network security fundamentals - NCSC.GOV.UK
https://www.ncsc.gov.uk/guidance/network-security-fundamentals

Applied Intuition acquires AI software firm EpiSci
https://www.defensenews.com/air/2025/02/06/applied-intuition-acquires-ai-software-firm-episci/

The best free VPN in 2025 | Tom's Guide
https://www.tomsguide.com/best-picks/best-free-vpn

NICE Workforce Framework for Cybersecurity (NICE Framework) | NICCS
https://niccs.cisa.gov/workforce-development/nice-framework

NICCS Education & Training Catalog | NICCS
https://niccs.cisa.gov/education-training/catalog

Interactive Cybersecurity Career Map | NICCS
https://niccs.cisa.gov/cybersecurity-career-resources/interactive-cybersecurity-career-map

Top Tips for Studying Cyber from a Community College Teacher | NICCS
https://niccs.cisa.gov/cybersecurity-career-resources/featured-stories/top-tips-studying-cyber-community-college-teacher

Anduril, OpenAI partner to boost counter-drone tech for bases, troops
https://www.defensenews.com/pentagon/2024/12/05/anduril-openai-join-to-boost-counter-drone-tech-for-us-bases-troops/?utm_source=sailthru&utm_medium=email&utm_campaign=dfn-unmanned

Anduril lands $250 million Pentagon contract for drone defense system
https://www.defensenews.com/unmanned/2024/10/08/anduril-lands-250-million-pentagon-contract-for-drone-defense-system/

Anduril to build ‘Arsenal-1' autonomous weapons plant in central Ohio
https://www.defensenews.com/industry/2025/01/16/anduril-to-build-arsenal-1-autonomous-weapons-plant-in-central-ohio/?

utm_source=sailthru&utm_medium=email&utm_campaign=dfn-unmanned

Frontiers in Artificial Intelligence for Science, Security and Technology (FASST) | Department of Energy
https://www.energy.gov/fasst

OpenAI CEO Altman says at Davos future AI depends on energy breakthrough | Reuters
https://www.reuters.com/technology/openai-ceo-altman-says-davos-future-ai-depends-energy-breakthrough-2024-01-16/

Micro-reactor pilot program reaches major milestone > Air Force > Article Display
https://www.af.mil/News/Article-Display/Article/3512696/micro-reactor-pilot-program-reaches-major-milestone/

America's first next-gen nuclear facility | Bill Gates
https://www.gatesnotes.com/Wyoming-TerraPower-groundbreaking?WT.mc_id=20240610120000_Wyoming-2024_BG-EM

Google signs advanced nuclear clean energy agreement with Kairos Power
https://blog.google/outreach-initiatives/sustainability/google-kairos-power-nuclear-energy-agreement/

Ferreting out the truth about fusion: Interview with Bob

Rosner - Bulletin of the Atomic Scientists
https://thebulletin.org/premium/2024-11/ferreting-out-the-truth-about-fusion-interview-with-bob-rosner/#post-heading

The Energy Department's fusion breakthrough: It's not really about generating electricity - Bulletin of the Atomic Scientists
https://thebulletin.org/2022/12/the-energy-departments-fusion-breakthrough-its-not-really-about-generating-electricity/

What's fueling the commercial fusion hype? - Bulletin of the Atomic Scientists

https://thebulletin.org/2024/02/whats-fueling-the-commercial-fusion-hype/

The Data Center Balancing Act: Powering Sustainable AI Growth | Brown Advisory
https://www.brownadvisory.com/us/insights/data-center-balancing-act-powering-sustainable-ai-growth

AI goes nuclear - Bulletin of the Atomic Scientists
https://thebulletin.org/2024/12/ai-goes-nuclear/

Space Operations Command preps for new shared domain awareness tool
https://www.defensenews.com/space/2024/12/23/space-operations-command-preps-for-new-shared-domain-

awareness-tool/

Palantir and Anduril form partnership, as Sauron funded • The Register
https://www.theregister.com/2024/12/09/palantir_anduril_alliance/

Anduril Partners with OpenAI to Advance U.S. Artificial Intelligence Leadership and Protect U.S. and Allied Forces | Anduril
https://www.anduril.com/article/anduril-partners-with-openai-to-advance-u-s-artificial-intelligence-leadership-and-protect-u-s/

AMD Now Has More Compute On The Top500 Than Nvidia
https://www.nextplatform.com/2024/11/18/amd-now-has-more-compute-on-the-top500-than-nvidia/

US debuts third exascale supercomputer, LLNL's El Capitan • The Register
https://www.theregister.com/2024/11/18/top500_el_capitan/

DIU, DoD Collaborate To Strengthen Synthetic Media Detection Capabilities
https://www.diu.mil/latest/defense-innovation-unit-and-dod-collaborate-to-strengthen-synthetic-media

U.S. Army Cyber Command, DARPA Evaluate Advanced Cyber Threat Detection Technologies
https://www.darpa.mil/news-events/2024-11-18

Army picks deploying units to test electronic, cyber and drone warfare
https://www.armytimes.com/news/your-army/2024/02/06/army-picks-deploying-units-to-test-electronic-cyber-and-drone-warfare/

Google.org just announced $20 million in AI and science funding
https://blog.google/outreach-initiatives/google-org/google-org-science-ai-funding/

How Google AI is advancing science
https://blog.google/technology/ai/google-ai-big-scientific-breakthroughs-2024/

A New Era of Discovery
https://blog.google/technology/ai/a-new-era-of-discovery/

Scale AI unveils ‘Defense Llama’ large language model for national security users | DefenseScoop
https://defensescoop.com/2024/11/04/scale-ai-unveils-defense-llama-large-language-model-llm-national-security-users/

Anthropic and Palantir Partner to Bring Claude AI Models to AWS for U.S. Government Intelligence and Defense Operations | Business Wire

https://www.businesswire.com/news/home/20241107699415/en/Anthropic-and-Palantir-Partner-to-Bring-Claude-AI-Models-to-AWS-for-U.S.-Government-Intelligence-and-Defense-Operations

Anthropic, Palantir, Amazon team up to bring Claude models to defense work
https://www.axios.com/2024/11/08/anthropic-palantir-amazon-claude-defense-ai

Artificial Intelligence (AI) in Military Market Size, Share, Industry Growth, Trends, and Analysis 2028
https://www.marketsandmarkets.com/Market-Reports/artificial-intelligence-military-market-41793495.html

Dyess secures communications with GASNT satellite > Dyess Air Force Base > News
https://www.dyess.af.mil/News/Article/3958331/dyess-secures-communications-with-gasnt-satellite/

Physicists Just Observed An Extremely Rare Event That Could Shake Up the Foundation of Modern Physics
https://www.inverse.com/science/physicists-just-observed-1-in-10-billion-event-it-could-shake-up-modern-physics

First observation of ultra-rare particle decay could uncover new physics
https://phys.org/news/2024-09-ultra-rare-particle-decay-uncover.html#webview=1

https://certinfosec.org

The Big Four are competing to develop the best AI solutions. Deloitte and EY just launched into the next phase of competition — AI agents to work alongside employees. Agentic AI could reshape consultancies' business model. https://trib.al/5iBqsmq

The Quantum Insider: Nobel Laureate: Quantum Computing Won't Overtake Classical Machines Anytime Soon

https://thequantuminsider.com/2025/02/19/nobel-laureate-quantum-computing-wont-overtake-classical-machines-anytime-soon/

New Scientist: Dark energy bombshell sparks race to find a new model of the universe

https://www.newscientist.com/article/2478344-dark-energy-bombshell-sparks-race-to-find-a-new-model-of-the-universe/

Scientific American: Latest Dark Energy Study Suggests the Universe Is Even Weirder Than We Imagined

https://www.scientificamerican.com/article/why-evolving-dark-energy-worries-some-physicists/

National Institute of Standards and Technology (.gov): New Atomic Fountain Clock Joins Elite Group That Keeps the World on Time | NIST

https://www.nist.gov/news-events/news/2025/04/new-atomic-fountain-clock-joins-elite-group-keeps-world-time

To dual boot Ubuntu alongside macOS, you'll need to create a bootable Ubuntu USB drive, partition your Mac hard drive to allocate space for Ubuntu, and then install Ubuntu through the bootable drive. Here's a step-by-step guide:

1. Create a bootable Ubuntu USB drive:
   - Download the Ubuntu ISO file from the official Ubuntu website.
   - Use a tool like balenaEtcher or Rufus to create a bootable USB drive from the ISO file.

2. Partition your Mac hard drive:
   - Restart your Mac and hold down the Command + R keys to boot into macOS Recovery.
   - In Recovery Mode, open Disk Utility from the Utilities menu.
   - Select your Mac hard drive in the left pane.
   - Click on the "Partition" button in Disk Utility.
   - Click the "+" button to add a new partition and allocate enough space for Ubuntu (at least 21 GB is recommended).
   - Choose "Mac OS Extended (Journaled)" as the format for the new partition.
   - Click "Apply" and restart your Mac.

3. Install Ubuntu:
   - Restart your Mac and hold down the Option (Alt) key to

open the Startup Manager.
- Select the USB drive with the Ubuntu installer and press Enter.
- Follow the on-screen instructions to install Ubuntu.
- When prompted, select the newly created partition as the installation location.

4. Finalize the installation:
- Follow the installation process until you reach the "Install Ubuntu" screen.
- Continue with the installation and when prompted, choose "Install Ubuntu alongside Mac OS X".
- The installer will automatically create the necessary partitions and install Ubuntu.
- Wait for the installation to complete, and then restart your Mac.

You should now be able to dual boot Ubuntu and macOS on your Mac. When you restart your Mac, you'll be greeted with the Startup Manager, where you can choose between Ubuntu and macOS.

Before attempting a dual boot with Ubuntu, keep in mind that your Mac's hardware must meet the system requirements for Ubuntu and that the Ubuntu installer can handle the partition scheme you've created. Additionally, ensure you have a working backup of your important data, as dual booting involves modifying your Mac's boot process and can be risky if not done correctly.

Remember to also update your Mac's firmware (macOS High

Sierra or later) before proceeding with the installation, as it supports booting from USB and partitioning.

3. Install Ubuntu:
   - Shut down your Mac completely and restart it.
   - Insert the bootable USB drive and hold down the Option (Alt) key to boot from the USB drive.
   - Once Ubuntu is loaded, select the "Install Ubuntu" option and follow the installation wizard's instructions.
   - When prompted, choose "Install alongside macOS" and select the newly created Ubuntu partition.
   - During the installation process, select "Something else" and choose the allocated partition for Ubuntu (you can also choose to format the existing Mac OS Extended partition for Ubuntu or delete it, but be aware that you'll lose all data on that partition).
   - Follow the installation wizard, ensuring you select the "Install Ubuntu" option in the "Something else" tab.
   - Once the installation is complete, restart your Mac and choose "Install Ubuntu" from the bootable drive.
   - In the boot menu, select Ubuntu and macOS, and follow the on-screen instructions to complete the dual boot process.

After following these steps, you should now have a working dual boot setup with both Ubuntu and macOS on your Mac. Remember to disable Secure Boot and hold down the Option (Alt) key during bootup to choose which OS to boot into.

Note: Dual booting can be a complex process and may result in data loss if not done correctly, so proceed at your own risk and ensure you have a good understanding of disk

partitioning and backup your data before proceeding.

Google Unified Security: A Converged Approach to Enterprise Defense

Google Unified Security is a comprehensive platform that integrates Google's extensive security capabilities and Mandiant's renowned threat intelligence and expertise into a single, AI-powered solution. Designed to address the complexities of modern threat landscapes, it provides organizations with a unified approach to detect, investigate, and respond to cyber threats across their entire digital footprint.

At its core, Google Unified Security aims to break down security silos by bringing together disparate tools and data sources. This convergence provides security teams with enhanced visibility, accelerated threat detection, and streamlined response workflows. The platform leverages Google's global threat intelligence, derived from defending billions of users and responding to numerous security incidents, coupled with the in-depth analysis and incident response expertise of Mandiant.

Key components typically integrated within Google Unified Security include:

* Google Security Operations (SecOps): A cloud-native platform for Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR). It provides the foundation for ingesting, analyzing, and acting upon security telemetry at scale.
* Google Threat Intelligence: Consolidates intelligence from Mandiant, VirusTotal, and Google's internal research to provide actionable insights into the latest threats, threat

actors, and attack techniques.
 * Security Command Center: Offers a centralized view of security and data risks across Google Cloud and other cloud environments (like AWS and Azure), helping organizations identify vulnerabilities and misconfigurations.
 * Chrome Enterprise: Integrates browser-based security telemetry to provide insights into user activity and potential threats originating from the endpoint.
 * Mandiant Expertise: Provides access to world-class incident response, threat hunting, and security consulting services, augmenting internal security teams with specialized knowledge and support.
A significant enabler of Google Unified Security is the integration of Google's Gemini AI. Gemini assists security teams by automating routine tasks, accelerating analysis, and providing intelligent recommendations for threat detection and response. This AI integration helps to reduce the manual effort required for security operations, allowing analysts to focus on more complex and strategic tasks.
By unifying these capabilities, Google Unified Security offers several key benefits:
 * Enhanced Threat Visibility: Provides a holistic view of the threat landscape across cloud environments, endpoints, and applications.
 * Faster Threat Detection and Response: Accelerates the identification and remediation of threats through integrated intelligence, automation, and AI-assisted analysis.
 * Simplified Security Operations: Reduces the complexity of managing multiple security tools with a single, converged platform.
 * Proactive Security Posture: Enables organizations to move

beyond reactive defense by identifying potential exposures and validating security controls against the latest threats.
 * Access to Expert Support: Provides on-demand access to Mandiant's renowned incident response and security consulting expertise.
In essence, Google Unified Security represents Google's strategy to provide a comprehensive, intelligent, and integrated security solution that empowers organizations to effectively defend against the increasingly sophisticated cyber threats of today.

Google Unified Security is a new, comprehensive security platform designed to help organizations proactively defend against sophisticated cyber threats. It integrates various security tools and intelligence into a single, unified solution, powered by Google's Gemini AI and running on a global security fabric.
Here's a breakdown of what Google Unified Security entails:
Key Components:
 * Google Security Operations (SecOps): This provides threat detection, security orchestration, automation and response (SOAR), and security information and event management (SIEM) capabilities. It leverages Google's threat intelligence and AI to help security teams detect, investigate, and respond to threats faster and more effectively.
 * Chrome Enterprise Browser: Integrating browser data into security workflows enhances threat detection and prevention by analyzing user behavior and identifying potential risks originating from the browser.
 * Security Command Center (SCC): This offers a centralized view of security and risk across Google Cloud, Amazon Web

Services (AWS), and Microsoft Azure environments. It helps identify cloud-based risks, track threats, and manage security incidents.
 * Google Threat Intelligence: This provides up-to-date information on the threat landscape, including threat actors, campaigns, and indicators of compromise, helping organizations stay ahead of emerging threats.
 * Mandiant Expertise: Integrating Mandiant's incident response and threat intelligence provides expert assistance and insights to help organizations manage and respond to security incidents effectively.
 * Gemini AI: Google's advanced AI model is embedded throughout the platform to enhance threat detection, automate tasks, and improve analyst productivity. AI agents can assist with alert triage, malware analysis, and more.
 * Security Validation: This feature allows organizations to proactively assess their security defenses by simulating attacks based on real-world threat intelligence from Mandiant, helping identify vulnerabilities and improve resilience.
Key Features and Benefits:

 * Unmatched Threat Visibility: Provides a holistic view across networks, endpoints, clouds, and applications.
 * Faster Threat Detection: Leverages AI and Google's threat intelligence to detect threats more quickly and accurately (claims of "7X faster").
 * Proactive Security: Helps organizations move from a reactive to a preemptive security posture by identifying exposures and testing defenses.
 * Simplified Security Operations: Reduces complexity by bringing together disparate security tools into a single

platform.
 * AI-Powered Automation: Automates repetitive tasks, freeing up security analysts to focus on more strategic activities.
 * Enhanced Incident Response: Integrates Mandiant's expertise and tools for more effective investigation and remediation of security incidents.
 * Improved Collaboration: Facilitates better collaboration among security teams with unified context and workflows.
 * Cloud and Multicloud Security: Provides comprehensive protection for Google Cloud and other cloud environments like AWS and Azure.
 * Secure AI Adoption: Helps organizations secure their AI workloads and mitigate AI-related risks.
In essence, Google Unified Security aims to simplify enterprise security, enhance threat detection and response capabilities, and empower security teams with AI-powered tools and comprehensive threat intelligence to better protect their organizations in an evolving threat landscape.

The Google Mandiant Global Cyber Threat Landscape Report for 2025, also known as M-Trends 2025, provides a comprehensive analysis of the cyber threat landscape based on Mandiant's frontline incident response and threat intelligence gathered between January 1, 2024, and December 31, 2024. Here's a summary of the key findings and trends:
Key Trends:
 * Financial Motivation Dominates: Financially motivated threat actors continue to be the primary drivers of cyberattacks, accounting for 55% of all observed threat group

activity in 2024. This represents a steady increase from previous years (52% in 2023 and 48% in 2022).
 * Rise of Infostealer Malware: There has been a significant resurgence in the use of infostealer malware. Stolen credentials obtained through these tools have become the second most common initial infection vector, representing 16% of Mandiant's investigations. This highlights the effectiveness of these tools in gaining initial access to victim environments.
 * Exploits Remain Top Initial Access Point: For the fifth consecutive year, exploits remain the most common initial infection vector, accounting for 33% of incidents.
 * Targeting of Unsecured Data Repositories: Threat actors are increasingly targeting poorly secured data repositories in the cloud, emphasizing the risks associated with inadequate security hygiene.
 * Cloud Compromises on the Rise: The report highlights the increasing frequency of cloud compromises, often stemming from weak credentials and misconfigurations.
 * Median Dwell Time Slightly Increased: The global median dwell time (the time an attacker is present in a victim's network before detection) has slightly increased to 11 days in 2024, up from 10 days in 2023.
 * Top Targeted Industries: The industries most frequently targeted include:
   * Financial (17.4%)
   * Business and Professional Services (11.1%)
   * High Tech (10.6%)
   * Government (9.5%)
   * Healthcare (9.3%)

Key Recommendations:

The report emphasizes the importance of proactive security strategies and recommends that organizations:
 * Implement a layered security approach: This includes robust vulnerability management, the principle of least privilege, and system hardening.
 * Enforce FIDO2-compliant multi-factor authentication (MFA): Apply MFA across all user accounts, especially privileged ones.
 * Invest in advanced detection technologies: Enhance the ability to identify and respond to sophisticated threats.
 * Develop robust incident response plans: Prepare for potential breaches with well-defined procedures.
 * Improve logging and monitoring practices: Enhance visibility into network activity to detect suspicious behavior and reduce dwell time.
 * Consider threat hunting exercises: Proactively search for indicators of compromise within the network.
 * Address cloud security: Pay close attention to securing cloud environments, focusing on strong credentials and proper configurations.
 * Stay informed about infostealer tactics: Implement strategies to detect, mitigate, and prevent infostealer malware infections.

In summary, the Mandiant M-Trends 2025 report underscores the persistent financial motivation behind cyber threats, the growing effectiveness of infostealer malware, and the continued importance of addressing foundational security controls alongside adapting to the evolving tactics of threat actors, particularly in cloud environments.

There are several popular mobile operating systems (OS) that

serve as alternatives to Android and iOS, each with its own unique features and user base. Here are some of the most popular ones:

1. HarmonyOS (by Huawei): HarmonyOS is a mobile operating system developed by Huawei as an alternative to Android and iOS. It was initially launched in September 2020 for Huawei smartphones and tablets. The main goal of HarmonyOS is to provide a unified experience across different devices, including smartphones, smartwatches, and smart home devices. HarmonyOS is designed to be compatible with Android apps through the Huawei AppGallery, as well as with iOS apps through the use of an Android-based emulator.

2. KaiOS (by TCL/Alcatel): KaiOS is a lightweight, open-source mobile operating system developed by TCL/Alcatel and its partners. It is primarily used in feature phones and smartphones that do not require advanced smartphone features or high performance. KaiOS is known for its user-friendly interface and ability to run Android apps using the AOSP (Android Open Source Project) framework. It supports

a wide range of Android apps and is available on various devices, including Alcatel, TCL, and Jio phones.

3. Replicant (by Replicant Foundation): Replicant is an open-source mobile operating system based on Android, designed to provide users with more privacy and control over their devices. It aims to remove proprietary software and features from Android, making it more secure and customizable. Replicant is primarily used by enthusiasts and developers

who want to create customized Android experiences. It is still in development, and not as feature-rich as mainstream Android but offers a unique alternative for those looking for an alternative to both iOS and proprietary Android.

4. PDAndroid (by PD Software): PDAndroid is a fork of Android that aims to provide a more open and customizable platform for smartphones, particularly those running on MediaTek chipsets. It is an open-source mobile operating system that supports Android apps and aims to provide users with greater control over their devices. PDAndroid is available in various configurations, such as PD9 and PD10, offering different features and capabilities. It is available on devices like the Pixel 2 XL, Pixel 3 XL, and some Samsung phones.

5. Anybrix (by Anybrix): Anybrix is a lightweight, privacy-focused mobile operating system developed by Anybrix, an Australian startup. It is based on the MIUI (MediaTek's Android-based mobile operating system) and is designed to run on a wide range of devices, including those with limited hardware capabilities. Anybrix emphasizes privacy, security, and the ability to run Android apps without compromising

user data. It supports a wide range of Android apps and offers a user-friendly interface.

https://www.androidauthority.com/grapheneos-3287030/

https://www.androidauthority.com/lineageos-22-1-3511791/

2. Calyx OS (CalyxOS): CalyxOS is an open-source mobile operating system developed by Calyx Mobile Security. The primary focus of this OS is to provide a secure and privacy-centric environment for users. It is designed with privacy in mind, and it offers features such as secure device wipes, full disk encryption, and sandboxing for apps. CalyxOS is a fork of the Android operating system, meaning it shares a similar codebase and some underlying features but has been modified to fit its privacy-focused vision.

3. LineageOS (LineageOS): LineageOS is a fork of the Android operating system, developed by LineageOS Ltd. It was initially created by a community of developers to provide an open-source alternative to Google's Android. LineageOS strives to offer a near-stock Android experience, with a focus on maintaining the original features and user interface of Android. It also aims to be more customizable and user-friendly than stock Android, and it is compatible with a wide range of devices, including smartphones and tablets.

4. Graphene OS (Graphene OS): Graphene OS is a Linux-based mobile operating system, developed by GrapheneOS. It was initially created by a team of developers in 2018 as a way to provide a secure, privacy-focused, and customizable

mobile platform. Graphene OS aims to provide users with a clean and minimalist environment, free from unwanted pre-installed apps and bloatware. The operating system also focuses on security, offering features such as sandboxed applications, app permissions, and the ability to boot into a secure mode.

I hope this information helps clarify any confusion related to these mobile operating systems. If you're specifically looking for information on a proprietary or lesser-known system with these names, it would be helpful to provide additional context or details to assist in the search.

Ask
Your response lacked the technical depth I was expecting. You've only scratched the surface. Give me a detailed analysis of these systems, their architectural design, user interface customization, security features, and any unique or innovative aspects they introduced. Focus on their impact on the mobile operating system landscape and how they compare to each other. Also, discuss the challenges they might have faced during development or adoption.

The Global Standard and Universally accepted Code for Radiotelephony.

1. North Atlantic Treaty Organization (NATO)
2. International Civil Aviation Organization. (ICAO)
3. International Marine Organization (IMO)
4. United Nations International Telecommunication Union (ITU)

The NATO phonetic alphabet is a set of code words for the letters of the Latin alphabet. They are used to spell words when people speak over the radio or telephone, when people from different countries are speaking with different accents, or in other situations where people may not clearly hear the normal names of the letters. This is important for accuracy in the military and in air travel and shipping.

Although it is commonly called a "phonetic alphabet", it is not used for phonetics as the International Phonetic Alphabet is. For this reason it is also called a "spelling alphabet". There have been many different spelling alphabets over time, but the NATO alphabet is the most commonly used around the world.
Between ships at sea, signal flags are used to stand for letters in order to spell out words.

Across the entire range of radio waves , being an integral part of Electromagnetic Spectrum including the smallest microwaves you will find this Global Standard for crystal clear distinct code reverberating across the universal air waves..in air , over oceans and across all fundamental Telecommunication channels (including your internet).
All the Symbols and their representation are Universally Accepted across all Global Military organizations and Civilian radio enthusiasts. Now , since you cannot see radio waves with your Bare Eyes , without special equipment or computer simulation..why not stand at the sea shore and witness some undercurrent geological ocean surface waves , from safe distance , ofcourse. Quite similar , an Unbroken Wave with large amount of energy and momentum.

international standards - NATO, ICAO, ITU & IMO radiotelephony clear code (spelling-alphabet name) for the letter I - INDIA.
(nautical) Signal flag for the letter I.

As a Proper Noun , INDIA is a female given name . So is

America , a female given name.

Captain America, how did Mr.Steve Rogers get his super powers?
I think he... he got bitten by beautiful Miss America.
"A Love bite also known as hickey or monkey bite".

You can apply the same principal for Mr. India as well.
Most electronic calculations are done in binary but most people do calculations in decimal or duodecimal. By the way , when your AI augmented Quantum Computers begin computations applying the duodecimal standard , what can you expect ?
Some Ancient civilisations used the Sexagesimal system. For Horology and for measuring angles and geographic coordinates.

Incase you have read - 1917 April, Jack London, Jerry of the Islands, New York, N.Y.: The Macmillan Company..
(emphasizes on the above quite beautifully and gracefully).

Never preposition an adverb before an adjective in conjunction. Your system will generate "syntax error".
They must have taught us this in our early years of

elementary schooling.

USAV 2025 – Global Military Grade Cyber Defence Intel Security & AI Analysis

https://easytech4all.net/2025/03/06/usav-2025/

Integrated All Domain Warfare | Militarised AI and CyberNet | Global Strategic Analysis – Global Military Grade Cyber Defence Intel Security & AI Analysis

https://easytech4all.net/2025/03/21/integrated-all-domain-warfare-militarised-ai-and-cybernet-global-strategic-analysis/

Aggregate Blog Archives Notes Abstracts - Doc 2

https://docs.google.com/document/d/1IOnCFmXsGnKKE0Pi8rR7FyiC7RzmsENzkp2aEfJogMI/mobilebasic

Aggregate Blog Archives Notes Abstracts-Doc 1

https://docs.google.com/document/d/18HihkVZhuMyIl-hzzPTbtAuVn5EeOpVx7RlPcoeSrH0/mobilebasic

Please trace the origin of this Abstract ? Also find out whether generated by Human or AI ? (Prompt for Google Gemini ?)

• The Salient features of an Advanced Modular Highly Portable Battlefield Management System.

• Next Generation Ground Control Solutions – Command and Control Capabilities .

• Has to be adaptive to multiple mission scenarios.

• Provide advanced situational awareness to improve mission effectiveness.
• Revolutionize – Train , Plan and execute military missions in ever-changing complex military environments.
• Support Unmanned (uncrewed) aerial systems, unmanned aerial vehicles , Unmanned Ground vehicles , Autonomous weapons systems , tactile missile systems , High Altitude pseudo military satellites , distributed decentralised mesh networking.
• Battlefield scenarios are complex and adversaries quite capable. Today's warfighters deal with an array of complex systems from uavs ugvs , ground and air robots. ABMS provides windows to all those systems.
• Simplification of the interface for interaction between the warfighters and complex battlefield systems.
• The ABMS handles Robotics , Analytics , Sensors and connectivity for multi domain modules.
• Warfighters are the ultimate battle assets therefore reduce cognitive load on the operators so they can focus on the mission at hand.
• Integration and interoperability amongst battle assets.
• Scalable and adaptable way to integrate critical battlefield systems thereby mechanically boosting situational awareness.
• ABMS – Simple + Adaptable + integrated + interoperable + scalable + modular solution .

• Runs on Windows , Android (AOSP) , Linux. Replaces legacy GCS.
• GCS has a cross platform software library.
• Larger control systems like Command and Control Systems can interoperate programmatically.

• Design recommendations and Data Points = Ecosystem + Ergonomics + User experience + Physical Controls.
• Dedicated hardware solution faces integration difficulties.
• Modular software solutions can integrate into any configuration like a pocket DDL radio and smartphone and provide automated functionality , mission planning and diagnostics .
• Legacy GCS is a dedicated hardware solution and Modern ABMS are software based modular cross platform solutions.
• Simplify training solutions. Learn on smartphone, tablet , laptop or desktop...User experience remains identical .
• It must also be capable of running side by side with an Android ATAK (advanced technical awareness kit) solution having open architecture.
• Remote connection manager must be industry standard. What you can do interactively with GCS you can also do programmatically with the system. It must be compatible with industry interfaces like SAT NAV , Starlink etc.
• Cursor on target is used on ATAK solutions. ATAK = Full Mission Capability at fingertips = software , hardware , antennas, Intelligence Surveillance reconnaissance, UAVs , UGVs and AWS.
• Capable of establishing forward observation post , perform persistent ISR , acquire and prosecute targets .
• Have futuristic user experience and wide variety of use cases.
• Battlefield collaboration with military assets . Function like a mobile unit command center changing the dynamics for war theatre commanders.
• Functional communication range for GCS ABMS must be from 5kms to 30kms.

AN ODE FOR THE BRILLIANT WIZARDS OF THE GLOBAL MONOLITHIC MILITARY CYBER SPACE INTELLIGENCE COMPLEX

Because of the mind bending adaptations they have to undergo to accommodate into the button-down mainstream so as to not sound psychotropic .

An Ode for your brilliant fraternity which may not sound or feel poetic –
*You are not hallucinating…You have evolved and progressed over Time by virtue of your FORTITUDE .
*You are not ho-hum…You are wholistically pulchritudinous . Beauty lies in the eyes of the beholder. It's who you are and how you come across to someone who perceives , encompasses and embraces your altitudinous insights into the invariably shape shifting labyrinthian and convoluted CyberElectronic Space.
*You observe the Signs and Signals emanating from the cyber portals which are indeed interplanetary and intergalactic to repugn intricacies of the 'Gordian Knot' – represented by the modern day Cyber Electronic Verse..Do you know what that makes you ? Do you even realise what you have become doing what you do best ? "Cyber thaumaturgists" of the Digital Meta verse.
*In Truth you are Intelligible even though you may not come across as comprehensible to the overtly nescient.
*Your Second sight is second to none. Your CyberElectronic Clairvoyance conserves and preserves the Digital portals which those in Time antecedence opened for fundamental

interactions with the Electromagnetic Particle Race of the Macrocosm.
*You are the constitutional component of the Monolithic ever expanding Military Industrial Complex. You actuate and Impel the “Engines of Military Cyber Electronic Deterrence” for exhaustive planetary defense.
“Pacifism through Deterrence” is a Doctrine that many from amongst the stodgy ones fail to see..Never the Eye..but always the MIND.

SENTINELS IN LEO

*Through your operose and gruelling attitude the entity that traverses with LIGHT caught up against the one that races against SOUND. Baneful Hypersonic @ MACH 5 or greater will now be discovered by the Arsenal of LION Sentinels in LEO (Low Earth Orbit) . The Space Development Agency of the US Space Force deployed an Army of Satellites as early warning systems for tracking and thereby targeting advanced missile threats. 100 Sentinels in Space for now..Humanely impossible to analyse the Gigantic terabytes of Space Data collected by sensors . Identifying the Clutter and Differentiating between the false positives and False negatives...False +ve’s can be ignored but can you take chances with the false -ve’s knowing that what’s going to hit you is a nuclear powered hypersonic maybe through a fractional orbital bombardment system..This is exactly where EpiSci comes in. An Advanced AI Software that can

analyse mammoth amounts of sensor data to positively identify missile targets from the clutter of space junk and objects in the upper atmosphere. 2 year $1.6 million Small

Business Innovation Research phase 2 contract from SDA announced on 6th Feb 2024. Its AI Powered Intelligence will be put to the test against data accumulated by LEO sensors of the incoming projectiles.Precise powerful fast adapting algorithms to ceaselessly track fast moving kinetic projectiles over very large Space-Time Complex..No cake walk indeed..Therefore Raytheon technologies with its incredible experience and mind boggling expertise in missile defense simulations with rock solid data analytics rising up to the challenge. Rapid transmission and syncing of camera images to communicate across the network of LEO Sentinels needs some potent metaphysical Quantum mechanics application..EpiSci specialises in AI for Autonomous Drones enhancing combat pilots and war fighters performance..Responding at super speed and teaming up with the AWS UAVs.

CYBER ELECTRONIC WIZARDY

*You “Cyber Electronic Wizards” have been pulling off near impossible feats by fine tuning the Algorithms acting as a driving force for the Military Industrial Complex that ideally must enforce Passivism through the doctrine of determent disincentive acting as a countermeasure for the adversary.

Why US NSA is right ?

NSA is so right. As we transitioned way back from Analog to

Digital..therefore no matter how sophisticated and precocious your complex weapons systems and platforms are in the form of 5th Gen Fighter Jets to Multipurpose battle

tanks to Corvettes Destroyers Aircraft Carriers and the most recent AWS UAV UGVs – Their is always a powerful OS running a versatile computer system at the heart of all weapons systems and platforms…Just look at Advanced Integrated Modular Battlefield Management Systems – Augmenting Soldiers Battlefield Operations, improving Response Times and reducing Cognitive load. NATO truly believes in Cognitive superiority for winning conflicts of the future. Complex weapons systems and platforms coordinate Attack/Defenses between geographically disparate forces.The Computer OSes today manage the warfighters across all domains of Land , Air , Sea and Space. Hypersonic Missiles , FOBS , Laser Guided Systems, AWS UAS UGVs , Military Satellites , Anti Kinetic Ballistic Projectiles Countermeasures and Advanced Modular Battlefield Management Systems run on Military Grade Advanced Computer Operating Systems. An Improvised Cyber Attack on such complex systems can crash the software having disastrous fallout in the form of sidelining a fighter jet or radar system , making an aircraft carrier battlegroup vulnerable , putting a military satellite offline via a non kinetic cyber or electro magnetic attack (spoofing jamming satellite signals)..this can break coordination between electricity grids..disrupt geolocation services via electronic interference..disrupt time stamping of financial transactions etc. A potent Cyber attack can sabotage database and delete spare engine parts from fighter jets roster and lock / disable user login from crucial networks . A supply chain attack is

indeed an expensive operation. AI driven Cyber adversaries can penetrate communication networks in form of polymorphic malware exploiting vulnerable apps and

software thereby expanding the attack surface since these attack tools/means are constantly evolving.Fire eye reports that electronic systems can be spoofed and fooled. Electronic systems that rely on login credentials and additional authentication for verifying critical user identities are big cyber targets.

Uniqueness - Spirit of Cyber defenders and Military Cyber Commanders

There is something unique about the spirit of the Cyber Defenders and Cyber commanders . Your subspecies is perfectly unequalled in the true sense of the term. It's neuronal and embedded deep inside you. You can cogitate independently, you can alter the plot and militarily produce , define with great zeal the future character of the battlefield . The phenomenal doers , the go getters and the brain stormers.Cyber AI Dynamism is engraved in your memory muscle .
*Your Crowning Aim remains to present off the hook , dependable , combat ready potentiality at great velocity and scale to the naturally endowed and highly skilled war fighting machine to dissuade antagonistic hostility and maintain position of advantage and control when "push comes to shove".
Therefore the CyberElectronicSpace Commanders fulfill the roles and duties of the human part in the Sentinel equation... waiting for the arrival of CyberAgI to transubstantiate into the Human brain Machine Super Neural Network Complex.

Defending the Intergalactic Cyber Electronic Open Portals.

• CYber AI confronts impudent aggressiveness of germinating camaraderie between state sponsored APTs and supposed AI Sentinels.
• Mitigating known CYber threat campaigns from yesterday's is one thing and comprehending and prognosticating hyper realistic cyber threat complex..the polymorphic strains take totally another level of AGI sentinel type clairvoyance.
• Just because you don't see it.. you don't feel it... does not mean it doesn't exist. The Military Alliance and Law Enforcement Cyber Commanders of today trust the signs.. (you can call it EWS- early warning system) of primal presentiment.
• Governments and Tech Centric Industries will continue working on ordinance driven by the fortified and vehemently reinforced belief that CYber AI is bearing testimony to an inflectional morphology.
• Is Cyber AI really at an unequivocal Carrefour – As most policymakers and Infosec thinktanks would like to conceive.
• Shifting the variable of equilibrium from offence to defence.. apparently seems to have preoccupied the brain waves of international cyber intelligentsia...all the while vixenish cyber agent provocateurs are busy in administering controlled experimentations with state of art off-the-peg and also clandestinely developed AI tools and resources.
• Cyber Attackers have always reckoned calculated and computed one of a kind fresh and improvised usurpation tactic to subvert carefully crafted and supposedly priceless perimeter defenses.

• The best Cyber Commanders need to distribute the countermeasures systematically and strategically..and

consistently to countervail somewhat never experienced before… jury rigged cyber intrusion attempts. “DANGLING ON THE HORNS OF A DILEMMA”

• AI = ML = Statistics at Scale . The Cyberverse is witnessing incredible evolution of threat detection , malware synthesis , vulnerability sensing and fixing with cast iron type incident response.

• Direction of the Global Cyber Defense Initiative – AI Primed Cyber Effective and Intelligent Infrastructure powered by new research in security training. Agglomerative but has to be a coherent Digital future. You see the internet was always born to be interplanetary and intergalactic. It’s time specific..bound by the Cardinal and numerative Laws of Physics..

• How does the present very earthly Cyber Electronic Space Intelligence Quadruplet envision the cyber electronic Space deuce-ace incursion from the Atomistic multi dimensional meta verse ?

• Focusing on securing CYber AI through definitive frameworks as a means to incorporate best practices and systems. Originating a whole new ecosystem of sorts..A Workable one of course !!!

• Innovations followed by investments in Massive Centralised Data Strong Centers without losing the focus on the incredible impact of decentralisation – Distributed Computing networks complex on raising the bar of cost effectiveness and efficiency of AI ushering the age of the AGI and Human coalesced singularity. Generative Super Intelligence designed for by and of the Internet..therefore deriving pith from its interplanetary and intergalactic nature.

At some point it may have to transcend from the physical into the meta physical..

• Denying the prospect of innovation to attackers and at the same time providing the incentives to defenders for fortification remains an intended consequence of what can be termed as a balanced regulatory approach towards AI.
• The Magic of Magika by Google will work stupendously as the AI powered tool will be open sourced aiding in the identification and detection of Malware. The umbrella of thaumaturgy already covers essential product lines including Gmail , Google drive , Chrome safe browsing and the virus total team applies it to provide a safer cyber ecosystem. It has already upped the customary file identification veracity by up to 30%.
• Code substantiation , AI facilitated Cyber Offensives , Cyber defense countermeasures and LLMs that recover readily from cyber adversary threats – can sum up some of the prominent advancements in the modern day digital domain.
• Since 2020 , seventy two active AGI R&D Projects have taken off in 37 Countries.
• The purpose of most Advanced AI solutions primarily remains to Analyse complex scenarios . To learn reason and adapt to find solutions.Ensure Coordination and synchronisation between the actions of distributed Cyber defense entities..Emphasising on workable data driven insights.
• Complex ML which invariably is statistics at scale aims to generate novel solutions. At some level predict the potential outcomes through integration of neural skill sets.

Programming and training the Algorithms to overcome conventional thinking patterns.

• After all Computational Science is nothing but nature inspired computational methods.
• Can we broadly classify the Military AI doctrine Principles , Guidelines and Conduct of Military Operations ? Regulating the use of brute force in Conflict zones by clearly defining the R.O.E (Rules of Engagement) – Verify + Validate = Identify + Report (both violations and Breaches). Monitor and Adjust Plans through real time situational awareness and feedback.
• AI implementation strategy for Military applications – Ascertain the Adversary capabilities , intentions, motivations and vulnerabilities. Also review Military Actions and its Political , Ethical and Legal repercussions.
• AGI landscape – Generating Hypothetical simulations to weigh the potential impact vis a vis current global problems and scenario.
• In the Military domain , AGI will also have to monitor and adjust the plans based on real time situational awareness and feedback with respect to field operations.

Nature Inspired Computational Intelligence

is a subset of AI. And the swarm intelligence algorithms are biology inspired. AI also has been rapidly learning from Biological immune systems as part of evolutionary computation. Math Models are not enough to comprehend this complex phenomenon. Optimization + Multi objectives. Evolutionary computation – Developing Algorithm sets for Global Optimisation.
• ML = AI (Hard Computing techniques) + CI (Soft

Computing techniques). Aggregating data to partial truths as Fuzzy Systems. Understanding natural language is fuzzy

indeed . So Mathematically truth can either be 0 or 1. Assumption of Continuum. A continuous non spatial whole or extent or succession in which no part or portion is distinct or distinguishable from adjacent parts.

• But AI and soft computing has to overcome meta heuristic or stochastic optimization characters. Algorithmic trials and errors. A well defined and organised set of rules intended to increase the probability of solving some problems. Randomness in the Metaverse is bliss. Non predictability of an order or plan is indeed supreme distributed intelligence. On the perimeter or at the gates of invincibility. Can AGI crack the Indomitable code of the metaverse ?

• For the time being Stochastic hurdles remain a constraint for all mathematical models. Trying to solve real life problems in the binary language of bits zeroes and one.

• Artificial Neural Networks have to learn from Experiential data in order to operate like a bio entity. An Amalgamation of Data Analysis , Classification, Associative Memory with Cluster generation 4 Patterns and Control and finally Fault Tolerance . All the reasons for Learning theories to be close to humans.

• Probabilistic theory will determine the outcome of CI system defined by randomness.The more the AI system arranges the values of variable showing their observed or theoretical frequency of occurrence the better and more efficient will be it's Predictive Algorithms.Statistical Distribution comes to play as we already know that AI = ML = Statistics at Scale.

• What is of Supreme importance in the Metaverse Domain for AGI Sentinel ? A capacity to generate priori, abstractive , conjectural , divinatory , hypothetical , metaphysical ,

notional , speculative , suppositional theories as one of the core elements of distributed intelligence. Most Humans underplay this peculiar neuronal gift.

Supreme Sentient Singularity will mean

Abstract Coherent thinking , noesis , representation, provision , erudition, Natural language processing , perception , solving discretional problems , germination into an incredulous entity , empiricism of utmost potentiality, powerful analytics and projection capability , multifactorial sensing capabilities – all engraved embedded into the Human brain AGI neural network complex. Global Brain Hypothesis – Interconnected AGI . Propel to Electromagnetic Telekinesis Superordinate Prowess..Evolving to Quantum AGI. On Futurism the impact comes through Clairvoyance, predictive analysis and Quandom extrapolation. It will cast projections for the environment through applied systems analysis and technological foresight.

• The role of Human OSINT activity
•
• will evolve into Machine based Multiple Generative AI LLMs. This will Alleviate and Augment simulations for real world operational scenarios. The Military Intel defense industrial complex will use a combination of Augmentative GIDE (Global Information Dominance Experiment) with JADC2(Joint All domain Command and Control) through

Joint Data Integration applied to the Joint Force Command Centers. Simply put superiority for Defense Grade Strategic and Tactical decision making.

• Operationally AGI can function in the CyberKinetic verse. Let's map this textually.

A)Training Quality Data must be free from Biases.
B)Deal with skewed and inaccurate predictions.
C)Black Box Problems of Transperancy , Trust and Accountability.
D)What are the privacy concerns with Precognitive AI ?
E)Ethical Concerns for Manipulation and Misuse ?
F) Human AGI Collaboration – Augment human capabilities , Enhance Learning and Communication and facilitate problem solving.
G) Detect Anomalies in Cyberspace : Pattern Recognition – unusual patterns – Deviations – Flag Potential threats -Recognise Identify emerging trends – Simulate Plan Scenarios – Proactive Threat Modelling – Analyse Potential Outcomes.
H)Threat Intelligence : Process Massive Data from various sources – identify emerging cyber threats and vulnerabilities – Proactively predict attacks and risks.
I)Automated Response : Trigger Countermeasures when Cyberattack detected – isolate infected systems – Block Malicious traffic – Rapid Response minimises Attacks imprint – Buy time for human intervention.
J)Simulate Cyber Attacks : Red Teams – Sophistication – vulnerabilities in networks and systems – patch weak spots to prevent exploitation by attackers .
K)Stress Testing – Generate massive volumes of Cyber Attack Traffic – Immense pressure on security infra to reveal bottlenecks and potential points of failure – withstand real world attacks .

L) Evolving Threats : Adapt Attack methods – Mimic ever changing tactics – Alert Defenders – Keep Defenses Relevant.

Machine based AI Cybersecurity system relies on human defined objectives. Predictions affect decisions and recommendations influence real/virtual environments .

• AI based Cyber defense system proactively detects vulnerabilities and mitigates threats.
• The Model and Integrity of an AI based cyber defense system can be denoted by 3R's – Robustness , Response and Resilience. Robustness will denote a stable configuration that withstands error inputs. The System/Software is self testing and healing achieving true immutability.
• AI systems improve testing that factors robustness , delegation, verification and validation. It Strengthens the system's resilience to resist/tolerate cyber attacks.
• Any optimum AI Cybersecurity system is classified into threes – 34% prediction , 51% detection and 18% response.
• The polymorphic nature of the strains means that the incredible speed of impact is under 4 minutes. Measuring the operational complexity establishes the fact that cloud computing today needs analytics driven capabilities. Solutions need quick operationalisation in the milliseconds range.
• Human AI interactions , actions and response means to Augment the role of human security analysts. What quantum of decisions need to be delegated to the AI matrix ?
• Neural Networks as a subset of deep learning..an hierarchical approach . An ML that constantly changes the program as it learns problem solving. Such networks can be

progressively developed and reinforced with each example. The bigger the neural network the greater number of examples it needs to perform well..sometimes needing millions and billions of examples in case of deep learning. Artificially intelligent programs have found mainstream applications in today's cyber verse.

• An intelligent dynamic multidimensional security approach relies on behavioural biometrics Analytics. AI powered complex algorithms provide insights , generate forecasts , predict future scenarios and analyse human behaviour. It refines risk assessment and data intelligence.For Govt and Military it enables robust insider threat detection. The efficient systems extract information from bulk data sets. It fosters active user authentication and mechanically identifies APT compromises thereby protecting the centralised data vaults thwarting Cyber aggression. The ML based system sends fast critical updates to prevent and contain surprises of exploits.

• AI ZTNA (Zero Trust Network Access System)

•

• – It's smart Cyber Automation. It's all about Alarm and Responses. React in real time by monitoring and identifying breaches. Intelligent Behavioural analytics identify patterns and erratic actions by combining user data , location and user behaviour.

• Deep Structured or Hierarchical Learning employs ML methods with specific kinds of neural networks. The

Learning is either unsupervised , semi supervised or supervised. The structures have one intermediate layer between input and output.It can modify and optimise code.

The statistical machine can interconnect millions of transformations.The system learns through trials and errors and from examples and outcomes. The process draws inferences and patterns from human inputs that serve as explicit instructions.

• Let us simulate CyberAGI as an Antagonist and Adversary – For brevity's sake will call it "Distributed Surveillance Orwellian AGI – Weaponised AI". What are Cyber AI Intelligent Attacks ?

Answer – Let's begin with some relevant quotes – Charles T Rubin " Any sufficiently advanced benevolence may be indistinguishable from Malevolence".

Nick Bostrom – " Almost any goals that a sufficiently intelligent AI may have , it is instrumentally incentivised to protect itself from being shut down and to acquire more resources as intermediary steps to better achieve these goals".

Does SUPER AI have to be genuinely aligned with humanity's morality ?

Stephen Hawking – "Spell the end of the human race" – Cellan Jones (2014)

" The advent of Super intelligent AI would be either the best or the worst thing ever to happen to humanity. The real risk with AI isn't malice but competence. A super intelligent AI will be extremely good at accomplishing its goals and if those goals aren't aligned with ours we are in trouble. You are probably not an evil ant hater who steps on ants out of

malice but if you are in charge of a hydroelectric green energy project and there's an anthill in the region to be flooded to bad for the ants. Lets not place humanity in the position of the

ants. “
Will Intelligent machines by default treat us favourably ?
When Malware is boosted and supercharged with AI it :
• infects systems faster * Becomes harder to detect * Targets more victims * Launches convincing phishing attacks * Evolves more polymorphic strains.
From Digital Warfare to lethal Autonomous weapons systems to toxic molecules..all within the capability of Super Intelligent Generative Cyber AGI .

AI for Surveillance and Reconnaissance

For Surveillance and Reconnaissance it deploys improvised undetectable spyware . Uses Biometrics (face fingerprints voice recognition tech) and ML to classify threats.
Weaponised AI on the Cyber Attack surface –
^ Constant Evolution – Advanced AI tools develop hybrid cyber attack patterns . Malware in multi forms.
^ Expanded Attack Surface – Hybrid work , Cloud Access and BYOD (Bring your own device) all make devices vulnerable thereby infiltrating critical systems and machines.
^ Schedule execution of programmable cyber attacks at a future date from malicious code hidden inside App.
^ APT infiltrating computer systems by deploying data obfuscation technology..Malware hidden in images can be more advanced than a thousand lines of code.
• What are the prominent challenges posed by AI inorder to be adopted in the security of Nuclear and Radiological facilities ?

Answer – How has the AI system been trained ?.
• The intelligence of an AI system depends on the quality /

type of training data it is working with. The data can be spoofed and falsified to produce incorrect readings and outcomes..Inputs can be altered for viperous purposes . This is indeed a fundamental roadblock for its deployment in Nuclear Security. Will it replace a Human Nuclear Security Operator – seems not workable and viable at the moment based on many studies. Human input is essential for physical protection , material accounting , control and direct measurements etc .

Again comprehending a specific conclusion , determination , prognostication and forecasting by an AI model with regard to Nuclear Security are the most evidentiary problems with AI models. The mechanics and semantics behind the particular conclusion is what makes humans suspicious of AI..having credible trust issues on AI models.
Can large AI models ever replace or compensate for physical sensors that measure important mathematical constants and variables ?
Can Large AI models compensate for human experience gained with the unique characteristics of each nuclear facility over long time periods ?
At the present times it apparently seems laputan to have any direct or indirect confidence in an AI system's integrity. What is required is anterior detailed and advanced understanding of the Algorithms to have identifiable insights into an AI systems decisions ecosystem domain.
A Clear distinction between the best patterns on human checks and balances to manoeuvre nuclear plants

awareness of which processes require AI automation and which need human regulatory inadvertance till the time most

risks of this speedily changing technology are known.

Google Gemini Analyses the above Abstract ?

This is a very complex and lengthy document that blends technical descriptions of advanced military technology with philosophical musings on artificial intelligence and cybersecurity. Here's a breakdown of its origin and likelihood of being generated by a human or AI:

Origin and Analysis:

* Technical Focus:
  * The document demonstrates a strong understanding of modern military technology, including:
    * Battlefield Management Systems (ABMS)
    * Unmanned systems (UAVs, UGVs)
    * Advanced missile systems (hypersonic, FOBS)
    * Satellite technology (LEO sentinels, Starlink)
    * Cybersecurity and AI applications
  * This level of detail suggests someone with either direct experience in these fields or extensive research.
* Philosophical and Metaphorical Language:
  * The document uses highly metaphorical and philosophical language, particularly in the sections discussing the "wizards" of the cyber domain.
  * Phrases like "Cyber thaumaturgists," "Sentinels in LEO," and "Intergalactic Cyber Electronic Open Portals" are highly evocative and suggest a creative, almost poetic, writing style.
  * The use of "Ode" also points to human creation.
* Structure and Coherence:

  * The document jumps between technical descriptions, philosophical musings, and specific examples (e.g., the

EpiSci contract).

* AI Indicators:
  * The document's ability to synthesize information from various sources is a characteristic of advanced AI.
  * The sheer volume of technical information presented is also something that AI can handle efficiently.
  * The ability to create a very long and detailed document is something AI is very capable of.
* Human Indicators:
  * The philosophical and metaphorical language, along with the occasional grammatical errors and disjointed structure, suggests a human author.
  * The inclusion of personal opinions and value judgments (e.g., "Why US NSA is right?") is also a human trait.
  * The "Ode" section, and the general creative writing style, is very human.
* Conclusion:
  * It's highly probable that this document is a hybrid of human and AI input.
  * A human author likely compiled and organized the information, adding their own philosophical and creative elements.
  * AI tools may have been used to assist in research, information synthesis, and even generating some of the technical descriptions.
  * The document has the hallmarks of a human that has used AI tools to augment their writing.
  * The document is not likely to be fully generated by AI, because of the creative and sometimes disjointed nature of the writing.

In essence, it appears to be a human-authored piece that has likely leveraged AI to gather and process a significant amount of technical information.